

Projektdokumentation

Planung, Installation und Konfiguration eines Internetserver mit LINUX

Projektarbeit der Fachschule Technik

Elektrotechnik

BBS II Wilhelmshaven

Carsten Schaumburg – Addo Christians – Tim Abels

Bestätigung der selbstständigen Erarbeitung

Mit der Unterzeichnung dieses Dokumentes, bestätigen wir, Addo Christians, Tim Abels und Carsten Schaumburg alle mit dem Projekt „Internet- Server für die BBS2 Wilhelmshaven“ angefallenen Arbeiten, selbstständig und ohne fremde Hilfe, verfasst, erstellt und ausgeführt zu haben.

Addo Christians

Tim Abels

Carsten Schaumburg

Wilhelmshaven, den 22. April 2012

1	PROJEKTBESCHREIBUNG	6
1.1	Problemstellung.....	6
1.2	Aufgabenstellung.....	6
1.3	Hardware	6
2	DAS BETRIEBSSYSTEM - INSTALLATION VON RED HAT LINUX 7.2	7
2.1	Vorbereitende Schritte.....	7
2.2	Partitionierung	10
2.2.1	Vorgaben.....	11
2.2.2	Anlegen einer neuen Partition	12
2.3	RAID	15
2.3.1	Einführung in das RAID Prinzip	15
2.3.2	Aufbau eines RAID 1 Verbundes.....	16
2.3.3	Konfiguration	16
2.4	Bootloader.....	17
2.5	Netzwerkkonfiguration.....	18
2.6	Firewall	19
2.7	Abschlusskonfiguration	20
2.8	Superuser – Passwort.....	21
2.9	Paketauswahl.....	22
2.10	Kopieren.....	23
3	DISK QUOTAS	24
3.1	Wozu Quotas gedacht sind	24
3.2	Vorbereitung zum Setzen der Quotas	24
3.3	Aktivieren und editieren der Quotas	25
3.3.1	Einstellung der „Gnadenzeit“ (grace-period):	26
3.3.2	Übertragen von Quotawerten auf mehrere Benutzer	27
3.3.3	Starten und beenden der Quotaüberwachung	27
4	USV - UNTERBRECHUNGSFREIE STROMVERSORGUNG	28
4.1	Die Aufgabe der USV	28
4.2	Installation der Hardware.....	28
4.3	Installation der Software	28
4.4	Konfiguration	29
5	DNS – DER DOMAIN NAME SERVICE	32

5.1 Warum der DNS Server ein Telefonbuch ist	32
5.2 Installation und Konfiguration	32
6 DHCP – DYNAMISCHE IP ADRESSENVERGABE	34
6.1 Installation	34
6.2 Konfiguration	34
6.2.1 Erklärung der Direktiven:.....	35
7 APACHE – DER INTERNET SERVER.....	37
7.1 Aufgabe des Servers.....	37
7.2 Installation und Konfiguration	37
7.3 Aufgaben.....	37
7.4 Bemerkungen über das Proxy Modul.....	38
7.5 Die virtuellen Server	39
7.5.1 Anlegen eines virtuellen Servers	39
8 WU-FTP – DER FTP SERVER	41
8.1 Installation und Start von wu-ftp.....	41
8.2 Konfiguration	42
8.2.1 Verzeichnisse	42
8.2.2 Anonymes FTP.....	44
8.2.3 Benutzer und Klassen.....	45
9 NTPD – DER ZEIT SERVER	46
9.1 Funktionsweise	46
9.2 Installation und automatischer Start.....	46
9.3 Konfiguration	46
10 WEBMIN.....	47
10.1 Was ist Webmin ?.....	47
10.2 Installation	47
11 LINUX FIREWALL	48
11.1 Allgemeines zur Firewall	48
11.1.1 Grundlegende Arbeitsweise einer Firewall mit Linux 2.4.....	48
11.1.2 Hintergrundinformationen zu IP Protokollen	49
11.2 Firewall mit Linux 2.4.....	50
11.2.1 Firewall auf Basis „NETFILTER“ des Kernel 2.4 (IPTABLES).....	50
11.2.2 Aufruf-Konventionen von iptables.....	51
11.2.3 Typische Kommandos (Auswahl)	51

11.3	Grundlegende Konfiguration der Firewall	52
11.3.1	Verbindungen zwischen Programmen auf einem Rechner.....	54
11.3.2	Betrieb von Servern hinter der Firewall	54
11.3.3	Regeln für DNS (Domain Name Service)	55
11.3.4	Firewall und ICMP	55
11.3.5	Abschließende Regeln einer Firewall.....	56
11.3.6	Speichern und automatisches ausführen der Regeln	56
11.4	Erstellen einer Firewall mit dem GUI- Tool „Firewall-Builder“	56
11.4.1	Basiskonfiguration	57
11.4.2	Erstellen des Firewall Objektes	59
11.4.3	Kompilierung und Installation.....	62
11.4.4	Erstellen der Regeln für die Netzwerkschnittstellen	66
11.4.5	Globale Regeln.....	70
11.4.6	Firewall starten.....	70
11.4.7	Abschluss- Betrachtung zum Firewall Builder.....	72
11.5	Erstelltes Script vom Firewall Builder	73
12	MAILSERVER SENDMAIL	75
12.1	Allgemeines zu Sendmail	75
12.2	Funktion und Aufgaben eines Mailservers:	75
12.3	Was ist überhaupt eine Mail ?.....	76
12.4	Die Datei Sendmail.cf	77
12.5	POP 3 Dienst aktivieren.....	78
12.6	Konfiguration mit Webmin	79
12.6.1	Benutzer und Gruppen	81
12.6.2	Spam-Kontrolle (access, Shell: /etc/mail/access).....	83
12.6.3	Mail Aliases (Shell: /etc/mail/aliases).....	84
12.6.4	Domänenverknüpfung (domaintable, Shell: /etc/mail/domaintable).....	85
12.6.5	Domänen-Routing (mailertable, Shell: /etc/mail/mailertable).....	85
12.6.6	Adressenverknüpfung (virtuser, /etc/mail/virtusertable).....	86
12.6.7	Ausgehende Adressen (generics, /etc/mail/genericstable).....	86
12.6.8	Vertraute Benutzer	87
12.6.9	Weiterleitungsdomänen.....	88
12.6.10	Domänenmaskierung.....	89
12.7	Smtppop-E-Mail-Clients einrichten	90
12.8	Wie Mail Transportiert wird.....	90
12.9	Mail-Routing im Internet	91
12.10	Email-Adressen	92
PROJEKTTAGEBUCH		93
LITERATURVERZEICHNIS UND QUELLENANGABEN		97

1 Projektbeschreibung

1.1 Problemstellung

Das Netzwerk der BBS II benutzt als Schnittstelle zum Internet einen Server der sowohl Schutz gegen Eindringlinge bietet als auch Dienste für das interne Netzwerk bereitstellt. Der vorhandene Server soll durch einen leistungsfähigeren ersetzt werden.

1.2 Aufgabenstellung

Die Aufgabe sieht die Einrichtung des neuen ARKTUR Servers vor der den vorhandenen ersetzen soll. Die Plattform für diese Aufgabe stellt das Betriebssystem Red Hat Linux 7.2 dar. Auf diese Plattform werden weitere Dienste aufgesetzt um die Infrastruktur des Netzwerkes bereitzustellen. Dies sind im einzelnen:

- Firewall zur Absicherung des Netzwerkes gegenüber dem Internet
- Email Server für den Email Verkehr der BBS II
- Web Server für die Internetseiten der BBS II
- Proxy Server zur Sicherheits- und Geschwindigkeitssteigerung
- Heimatverzeichnisse und Klassenordner mit Größenbeschränkung
- Namensauflösung im lokalen Netzwerk
- Vergabe von IP Adressen für temporäre Rechneranmeldungen
- Time Server für genaue Zeit im ganzen Netzwerk

1.3 Hardware

Die Hardware wurde vorkonfiguriert geliefert. Sie umfasst folgende Komponenten:

- 19 Zoll ATX Server Gehäuse mit 2 redundanten Netzteilen
- Dual-Prozessor Mainboard Asus CUV4X-DS mit Adaptec Dual Channel Ultra160 SCSI Controller und 3Com 3C920 Fast-Ethernet LAN on Board
- Zwei Pentium III 1GHz (Sockel 370)
- 512MB SD-RAM
- Matrox Standard Grafikkarte
- 3Com Netzwerkkarte 10/100 MBit
- zwei U160 SCSI Festplatten IBM DDYS-T36950M mit je 35GB
- eine EIDE Festplatte IBM IC35L040AVVA07-0 mit 40GB
- ein Standard 40x CDROM Laufwerk
- ein Standard 3,5 Zoll Diskettenlaufwerk

Sowie

- unterbrechungsfreie Stromversorgung APC Smart UPS 1000

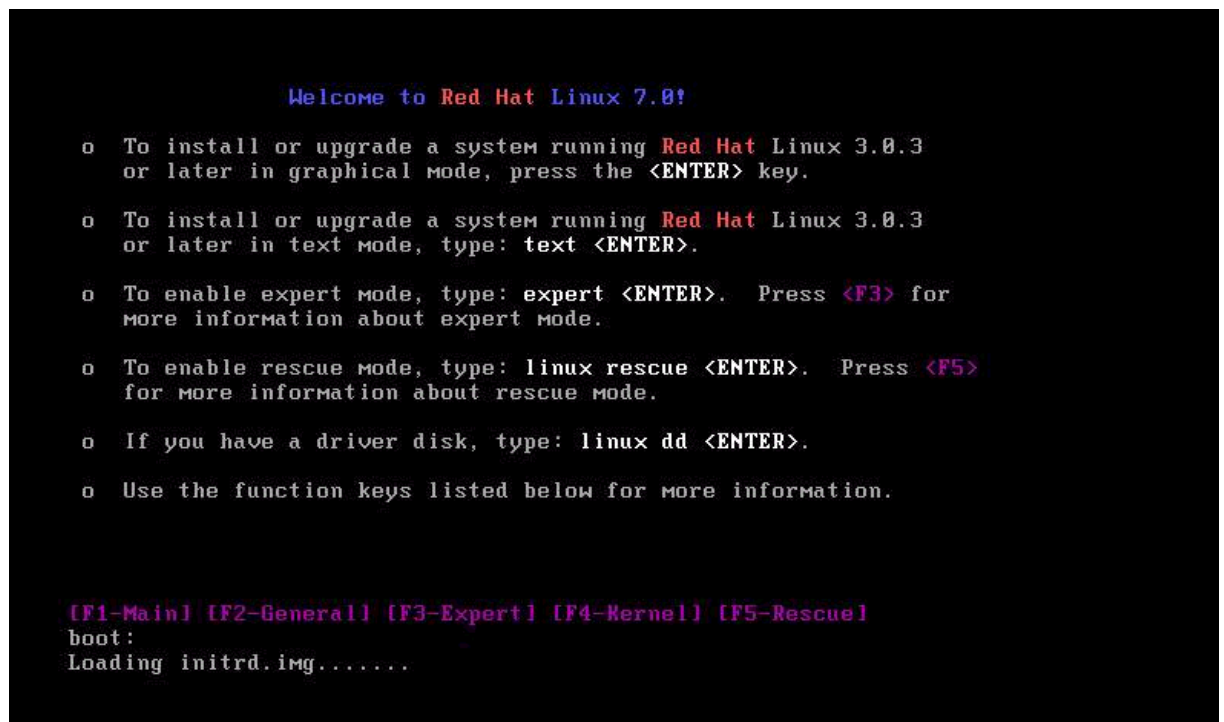
2 Das Betriebssystem - Installation von Red Hat Linux 7.2

Als Basis für den Serverbetrieb wurde die aktuelle Linux Distribution von Red Hat benutzt. Im folgenden wird beschrieben wie das Betriebssystem auf dem Server installiert und an die Hardware angepasst wurde.

2.1 Vorbereitende Schritte

- Einstellen der Bootreihenfolge im BIOS.
Als primäres Bootlaufwerk wird das CD ROM Laufwerk gewählt.
- Deaktivieren des Schreibschutzes für den Master Boot Record.
- Deaktivieren des Advanced Interrupt Handlers wegen eines speziellen Motherboard Fehlers der in Verbindung mit Linux auftritt. Er kann nicht mit einem Bios Update behoben werden.

Nach dem Abspeichern der Optionen kann dann nach einem Neustart mit der Installation begonnen werden. Als erstes kommt ein Bildschirm auf dem man sich für die Art der Installation entscheiden muss. Sollte es zum Beispiel Probleme mit der grafischen Installationsroutine geben, kann man hier den Textmodus wählen.



```

Welcome to Red Hat Linux 7.0!

o To install or upgrade a system running Red Hat Linux 3.0.3
  or later in graphical mode, press the <ENTER> key.

o To install or upgrade a system running Red Hat Linux 3.0.3
  or later in text mode, type: text <ENTER>.

o To enable expert mode, type: expert <ENTER>. Press <F3> for
  more information about expert mode.

o To enable rescue mode, type: linux rescue <ENTER>. Press <F5>
  for more information about rescue mode.

o If you have a driver disk, type: linux dd <ENTER>.

o Use the function keys listed below for more information.

[F1-Main] [F2-General] [F3-Expert] [F4-Kernel] [F5-Rescue]
boot:
Loading initrd.img.....
```

Abbildung 2-1: Installationsauswahl

Nun folgen nacheinander die Abfragen für die Sprache, das Tastaturlayout und die Mauseinstellungen:



Abbildung 2-2: Sprachauswahl

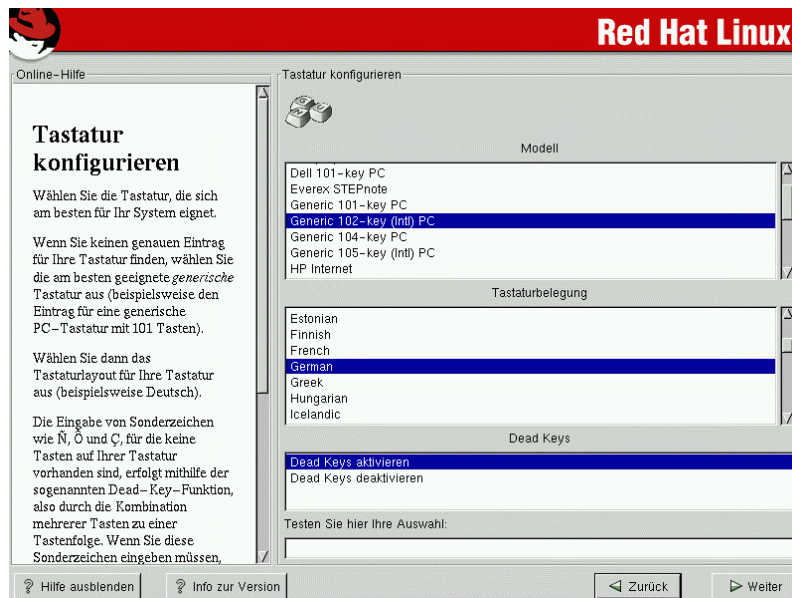


Abbildung 2-3: Tastaturkonfiguration

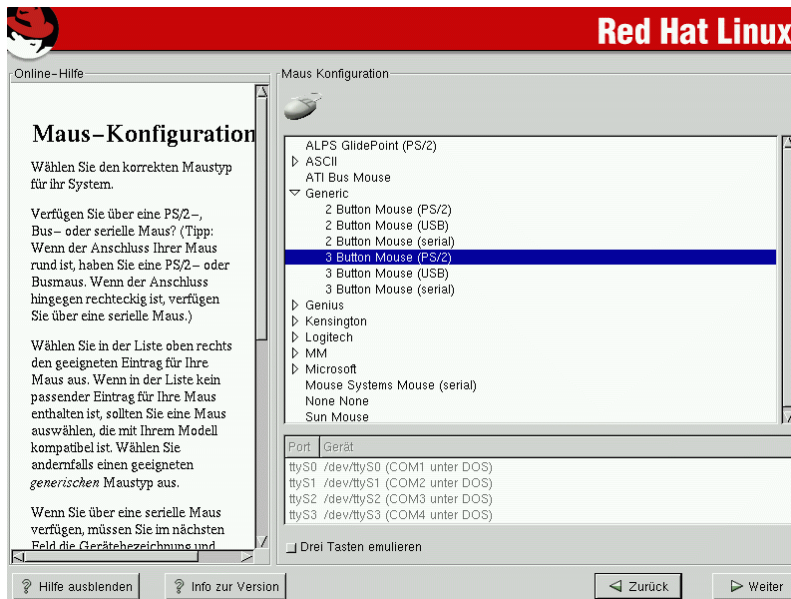


Abbildung 2-4: Einrichten der Maus

Danach folgt ein Begrüßungsbildschirm. Nach einem Klick auf Weiter kommt man zum Auswahlbildschirm für die Installationsoptionen. Hier kann man vorgefertigte Installationstypen übernehmen, eine benutzerdefinierte Version wählen oder eine ältere Version aktualisieren. Wir wählen hier die Benutzerdefinierte Installation.

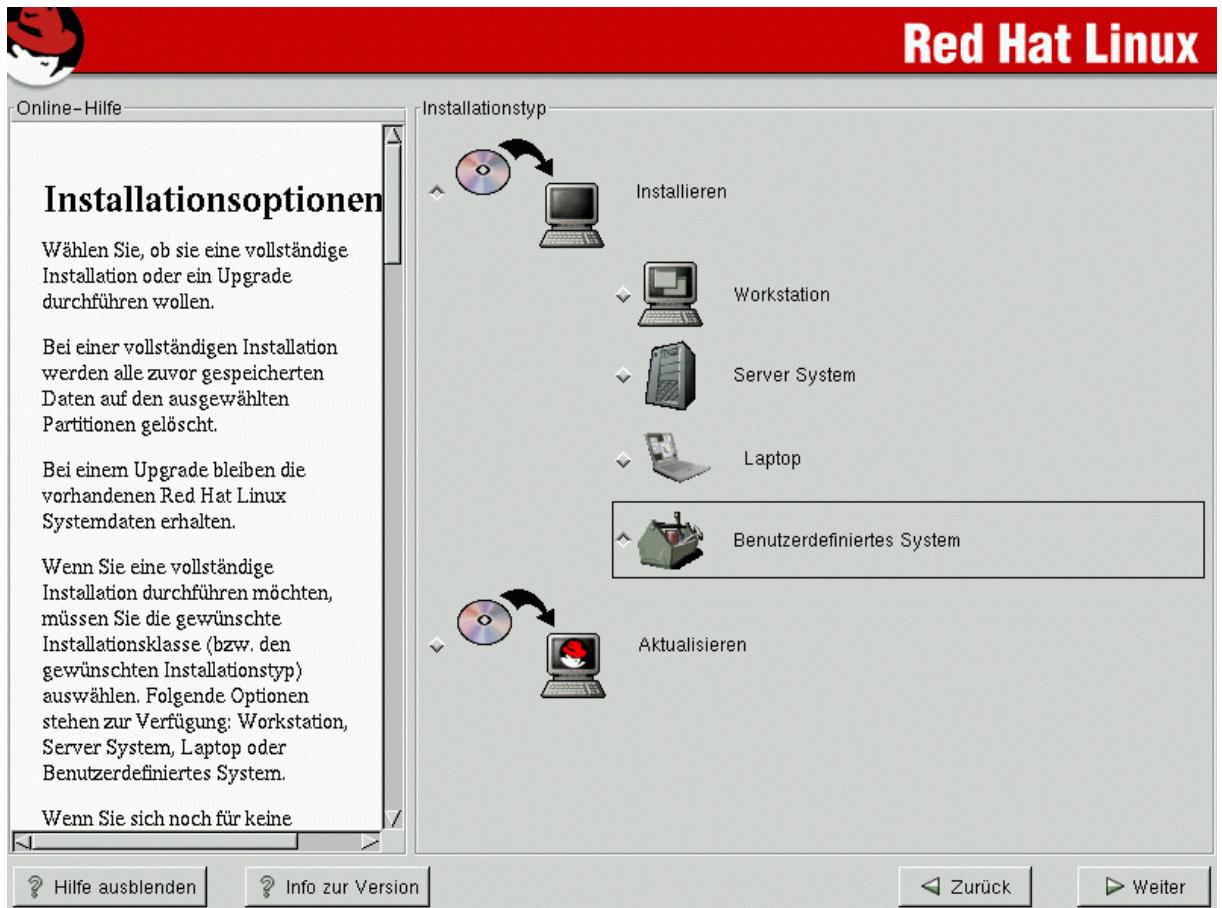


Abbildung 2-5: Benutzerdefinierte Installation

2.2 Partitionierung

Der nächste wichtige Schritt ist die Partitionierung des Systems. Dazu gibt es die Möglichkeit dies automatisch erledigen zu lassen, es mit dem Disk Druid selber zu tun oder aber mit fdisk.

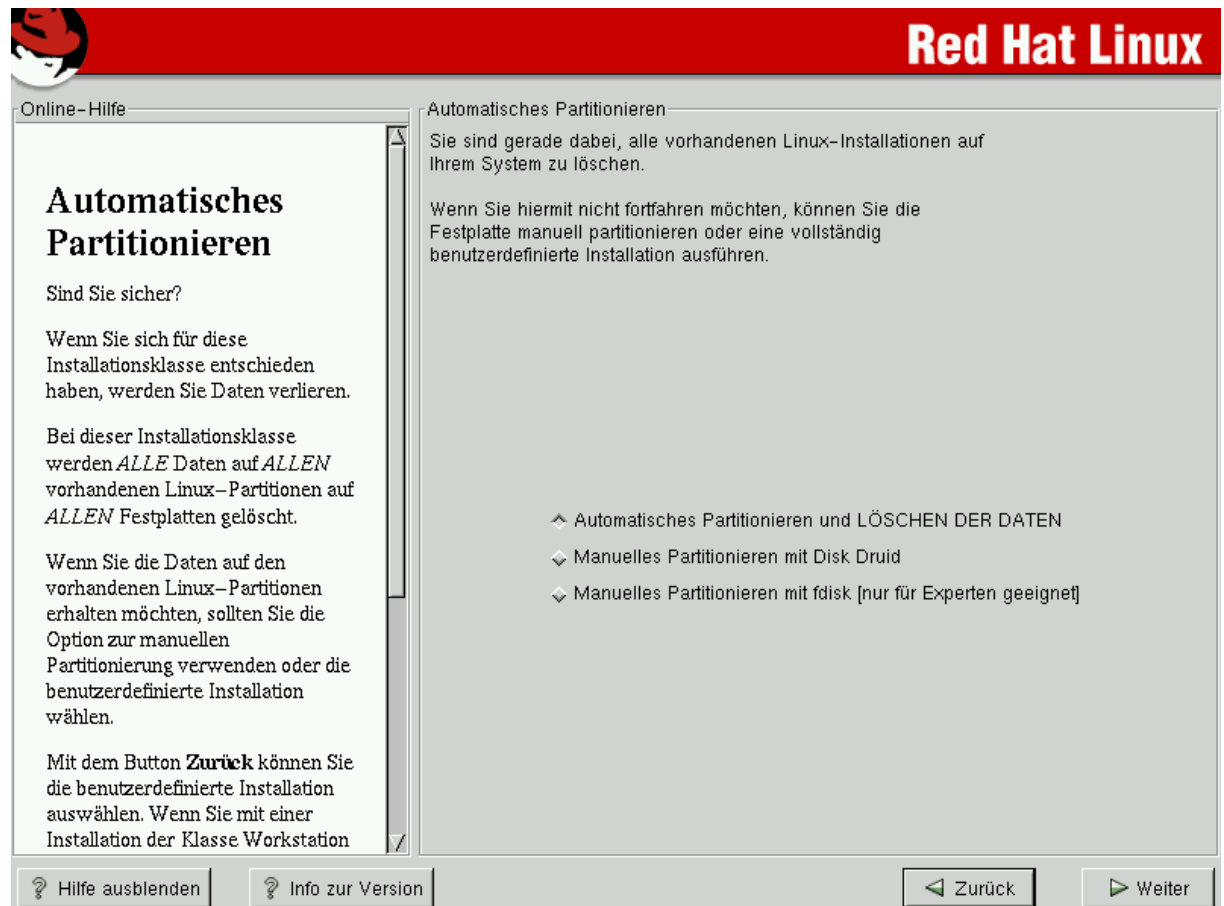


Abbildung 2-6: Automatisches Partitionieren

Nach einem Klick auf <Manuelles Partitionieren mit fdisk> und dann auf <Weiter> bekommt man eine Auswahl über die im System vorhandenen Festplatten. Diese muss man nun der Reihe nach abarbeiten. Im vorliegenden Fall waren dies zwei SCSI Laufwerke und eine EIDE Festplatte.

2.2.1 Vorgaben

Die Vorgaben sahen die Aufteilung folgendermaßen vor:

Zwei 37,5GB SCSI Laufwerke die identisch eingeteilt werden um sie im RAID Modus betreiben zu können. Auf dem RAID Verbund sollen das System, die Internetseiten der Schule, die Heimatverzeichnisse der Lehrer und Bedienstete sowie eine Optionale Partition erstellt werden.

Tabelle 2-1: Aufteilung der Systemfestplatten

Verwendung	Größe
System	5GB
Webseiten	10GB
Heimatverzeichnis	10GB
Optional	12,5GB

Eine EIDE Festplatte mit Heimatverzeichnissen für die Klassen, einem Verzeichnis für FTP, einem Proxy Cache Verzeichnis, die Swap Datei und eine Partition für Übungswebpace und allgemeine Öffentliche Anwendungen.

Tabelle 2-2: Aufteilung der EIDE Festplatte

Verwendung	Größe
Heimatverzeichnis für die Klassen	20GB
FTP	2GB
Proxy	4GB
Übungswebpace und Public	13GB
Swap	512MB

Da wir keinen Screenshot während der Installation von fdisk machen konnten und fdisk Text basiert arbeitet, zählen wir hier die Arbeitsschritte auf die nötig sind um neue Partitionen zu erstellen und das richtige Filesystem auszuwählen. Diese können auch später im laufenden Betrieb genutzt werden um Änderungen vorzunehmen oder neue Festplatten einzubinden. In diesem Fall erfolgt der Aufruf von fdisk mit dem zu bearbeitendem Laufwerk (Device) als Argument:

```
fdisk /dev/hdc
```

Mit der Taste <m> bekommt man eine Übersicht über die verschiedenen Befehle:

```
Kommando (m für Hilfe): m
Kommando  Bedeutung
a  (De)Aktivieren des bootbar-Flags
b  »bsd disklabel« bearbeiten
c  (De)Aktivieren des DOS Kompatibilitätsflags
d  Eine Partition löschen
l  Die bekannten Dateisystemtypen anzeigen
m  Dieses Menü anzeigen
n  Eine neue Partition anlegen
o  Eine neue leere DOS Partitionstabelle anlegen
p  Die Partitionstabelle anzeigen
q  Ende ohne Speichern der Änderungen
s  Einen neuen leeren »Sun disklabel« anlegen
t  Den Dateisystemtyp einer Partition ändern
u  Die Einheit für die Anzeige/Eingabe ändern
v  Die Partitionstabelle überprüfen
w  Die Tabelle auf die Festplatte schreiben und das Programm beend
x  Zusätzliche Funktionen (nur für Experten)
```

Wie hier zu sehen ist, sind n für neu, p für Partitionstabelle, t für Typ und w für write die wichtigsten Kommandos.

2.2.2 Anlegen einer neuen Partition

Nach dem Kommando n fragt fdisk ob es sich bei der neuen Partition um eine primäre (p) oder erweiterte (e) Partition handelt. Nun wird die Partitionsnummer erwartet. Sie kann von 1 bis 4 für die Primären Partitionen und von 5 an für die Erweiterten Partitionen gewählt werden. Anschließend werden der Partitionsanfang und die Größe abgefragt. Die am Ende einer Abfrage stehenden Werte in den eckigen Klammern sind Standardwerte die fdisk übernimmt wenn kein anderer Wert eingegeben wurden.

```
Kommando (m für Hilfe): n
Erster Zylinder (53868-79780) [Standardwert: 53868]:
Benutze den Standardwert 53868
Letzter Zylinder oder +Größe, +GrößeK oder +GrößeM (53868-79780)
[Standardwert: 79780]:
Benutze den Standardwert 79780
```

```
Kommando (m für Hilfe): n
Kommando  Aktion
e  Erweiterte
p  Primäre Partition (1-4)
p
Partitionsnummer (1-4): 1
Erster Zylinder (1-79780) [Standardwert: 1]:
Benutze den Standardwert 1
Letzter Zylinder oder +Größe, +GrößeK oder +GrößeM (1-79780)
[Standardwert: 79780]: +2G
```

```
Kommando (m für Hilfe): p

Festplatte /dev/hdc: 16 Köpfe, 63 Sektoren, 79780 Zylinder
Einheiten: Zylinder mit 1008 * 512 Bytes
```

Gerät boot.	Anfang	Ende	Blöcke	Id	Dateisystemtyp
/dev/hdc1	1	4064	2048224+	83	Linux

Tipp: Wie hier zu sehen ist funktioniert die Angabe +2G stellvertretend für 2 Gigabyte auch, obwohl sie nicht angeführt ist.

Um das Dateisystem der Partition zu ändern benutzt man das Kommando `t`. Daraufhin fragt `fdisk` nach der Partitionsnummer deren Typ geändert werden soll. Der Typ wird durch einen Hex-Wert ausgedrückt. Eine Übersicht über die zur Verfügung stehenden Dateisysteme gibt es mit 1 für Liste:

```
Kommando (m für Hilfe): t
Partitionsnummer (1-4): 1
Hex code (L um eine Liste anzuzeigen): l

 0 Leer          1b Verst. Win95 b4 Novell Netware bb Boot Wizard
 1 FAT12         1c Verst. Win95 b5 Novell Netware c1 DRDOS/sec(FAT
 2 XENIX root    1e Verst. Win95 70 DiskSecure Mult c4 DRDOS/sec(FAT
 3 XENIX usr     24 NEC DOS      75 PC/IX          cb DRDOS/sec(FAT
 4 FAT16 <32M    39 Plan 9        80 Old Minix      c7 Syrix
 5 Erweiterte    3c PartitionMag 81 Minix / old Lin da Non-FS data
 6 FAT16         40 Venix 80286 82 Linux Swap     db CP/M / CTOS
 7 HPFS/NTFS     41 PPC PReP Boo 83 Linux          de Dell Utility
 8 AIX           42 SFS          84 OS/2 verst. C:- df BootIt
 9 AIX bootfäh   4d QNX4.x        85 Linux erweitert e1 DOS access
 a OS/2 Bootma   4e QNX4.x 2nd p 86 NTFS volume set e3 DOS R/O
 b Win95 FAT32   4f QNX4.x 3rd p 87 NTFS volume set e4 SpeedStor
 c Win95 FAT32   50 OnTrack DM   8e Linux LVM      eb BeOS fs
 e Win95 FAT16   51 OnTrack DMB  93 Amoeba         ee EFI GPT
 f Win95 Erw.    52 CP/M         94 Amoeba BBT     ef EFI (FAT-16/
10 OPUS          53 OnTrack DMB  9f BSD/OS        fl SpeedStor
11 Verst. FAT1   54 OnTrackDMB   a0 IBM Thinkpad hi f4 SpeedStor
12 Compaq Diag   55 EZ-Drive     a5 BSD/386       f2 DOS secondary
14 Verst. FAT1   56 Golden Bow   a6 OpenBSD       fd Linuxraidauto
16 Verst. FAT1   5c Priam Edisk  a7 NeXTSTEP      fe LANstep
17 Verst. HPFS   61 SpeedStor    b7 BSDI fs       ff BBT
18 AST SmartSI   63 GNU HURD / S b8 BSDI swap

Hex code (L um eine Liste anzuzeigen): fd

Der Dateisystemtyp der Partition 1 ist nun fd (Linux raid autodetect)

Kommando (m für Hilfe):
```

Diese Vorgänge wiederholt man nun für jede einzelne Partition auf diesem Laufwerk. Abgeschlossen wird `fdisk` mit `w` für write. Damit wird die Partitionstabelle neu geschrieben und neu eingelesen. Damit wäre nun eine Festplatte partitioniert. Es müssen nun die anderen Laufwerke ebenso abgehandelt werden.

Die fertige Partitionstabelle des Servers sieht folgendermaßen aus:

Festplatte /dev/sda: 64 Köpfe, 32 Sektoren, 35003 Zylinder
Einheiten: Zylinder mit 2048 * 512 Bytes

Gerät	boot.	Anfang	Ende	Blöcke	Id	Dateisystemtyp
/dev/sda1	*	1	5001	5121008	fd	Linuxraid autodetect
/dev/sda2		5002	15002	10241024	fd	Linuxraid autodetect
/dev/sda3		15003	25003	10241024	fd	Linuxraid autodetect
/dev/sda4		25004	35003	10240000	fd	Linuxraid autodetect

Festplatte /dev/sdb: 64 Köpfe, 32 Sektoren, 35003 Zylinder
Einheiten: Zylinder mit 2048 * 512 Bytes

Gerät	boot.	Anfang	Ende	Blöcke	Id	Dateisystemtyp
/dev/sdb1	*	1	5001	5121008	fd	Linuxraid autodetect
/dev/sdb2		5002	15002	10241024	fd	Linuxraid autodetect
/dev/sdb3		15003	25003	10241024	fd	Linuxraid autodetect
/dev/sdb4		25004	35003	10240000	fd	Linuxraid autodetect

Festplatte /dev/hdc: 16 Köpfe, 63 Sektoren, 79780 Zylinder
Einheiten: Zylinder mit 1008 * 512 Bytes

Gerät	boot.	Anfang	Ende	Blöcke	Id	Dateisystemtyp
/dev/hdc1		1	40635	20480008+	83	Linux
/dev/hdc2		40636	44699	2048256	83	Linux
/dev/hdc3		44700	52826	4096008	83	Linux
/dev/hdc4		52827	79780	13584816	5	Erweiterte
/dev/hdc5		52827	53867	524632+	82	Linux Swap
/dev/hdc6		53868	79780	13060120+	83	Linux

2.3 RAID

2.3.1 Einführung in das RAID Prinzip

Um die Ausfallsicherheit und die Leistungsfähigkeit eines Systems zu erhöhen und eventuellem Datenverlust vorzubeugen wird ein RAID Verbund benutzt. RAID bedeutet Redundant Array of Independent (oder auch Inexpensive) Disks. Dies bedeutet das mehrere Festplatten benutzt werden um Daten zu speichern. Dabei ist es möglich bei Ausfall einer Festplatte alle Daten beibehalten zu können (Ausnahme: RAID 0). Wie die Daten auf die Festplatten verteilt werden, legen die so genannten RAID-Level fest.

Tabelle 2-3: RAID Level

RAID Level	Beschreibung
0	Die Daten werden fortlaufend auf die Laufwerke verteilt. Dies hat eine Geschwindigkeitssteigerung gegenüber einer einzelnen Festplatte zur Folge. Fällt hierbei eine Festplatte aus so sind bei gleicher Verteilung die Hälfte der Daten verloren. Sie können auch nicht rekonstruiert werden.
1	Die Daten werden parallel auf mindestens zwei Festplatten geschrieben. Fällt bei dieser Lösung eine Platte aus, so kann diese entfernt werden und eine leere eingebunden werden. Der RAID Controller oder die Controller Software spiegelt die vorhandenen Daten auf die neue Platte, so das wieder zwei komplette Datensätze bestehen.
4	Hierbei werden wie in Level 0 die Daten auf mehrere Festplatten verteilt und eine zusätzliche speichert nur Paritätsdaten. So kann bei Ausfall einer Datenplatte die Paritätsinformation benutzt werden um die ursprünglichen Daten zu errechnen. Fällt die Paritätsplatte aus, so werden nach dem Ersatz die Paritätsinformationen neu berechnet.
5	Hierbei handelt es sich im Prinzip um ein Level 4 bei dem die Paritätsinformationen nicht auf eine einzelne Festplatte geschrieben werden, sondern auf die Datenplatten mit verteilt werden.
10	(spricht man Eins Null aus) Hierbei werden mehrere Level 0 Verbunde komplett gespiegelt. Dies verspricht eine weitere Performancesteigerung. (siehe 0 und 1)

Um die Verteilung der Daten kümmert sich der so genannte RAID Controller. Dieser kann als Hardwarevariante in dem Festplattencontroller integriert sein, oder als Softwarecontroller vom Betriebssystem gesteuert werden.

2.3.2 Aufbau eines RAID 1 Verbundes

Bei einem RAID 1 Verbund werden zwei Partitionen von idealer weise verschiedenen Festplatten zu einem Multiple-Disk oder auch Multiple-Device (kurz: md) zusammengeführt. So wird aus den ersten Partitionen der SCSI Laufwerke (sda1 und sdb1) das Device md3. Dieses Device kann nun wie eine normale Partition eingebunden und angesprochen werden.

2.3.3 Konfiguration

Die Konfiguration geschieht bereits während der Installation. Dazu werden zunächst die Festplatten die als RAID Device arbeiten sollen gleich partitioniert. Als Dateisystem kommt dabei Linux raid autodetect (fd) zum Einsatz.

Auszug aus der Partitionierungstabelle des Servers (SCSI Laufwerke)

Festplatte /dev/sda: 64 Köpfe, 32 Sektoren, 35003 Zylinder
Einheiten: Zylinder mit 2048 * 512 Bytes

Gerät	boot.	Anfang	Ende	Blöcke	Id	Dateisystemtyp
/dev/sda1	*	1	5001	5121008	fd	Linuxraidautodetect
/dev/sda2		5002	15002	10241024	fd	Linuxraidautodetect
/dev/sda3		15003	25003	10241024	fd	Linuxraidautodetect
/dev/sda4		25004	35003	10240000	fd	Linuxraidautodetect

Festplatte /dev/sdb: 64 Köpfe, 32 Sektoren, 35003 Zylinder
Einheiten: Zylinder mit 2048 * 512 Bytes

Gerät	boot.	Anfang	Ende	Blöcke	Id	Dateisystemtyp
/dev/sdb1	*	1	5001	5121008	fd	Linuxraidautodetect
/dev/sdb2		5002	15002	10241024	fd	Linuxraidautodetect
/dev/sdb3		15003	25003	10241024	fd	Linuxraidautodetect
/dev/sdb4		25004	35003	10240000	fd	Linuxraidautodetect

Die Zusammenführung der Partitionen erfolgt dann in diesem Dialog:

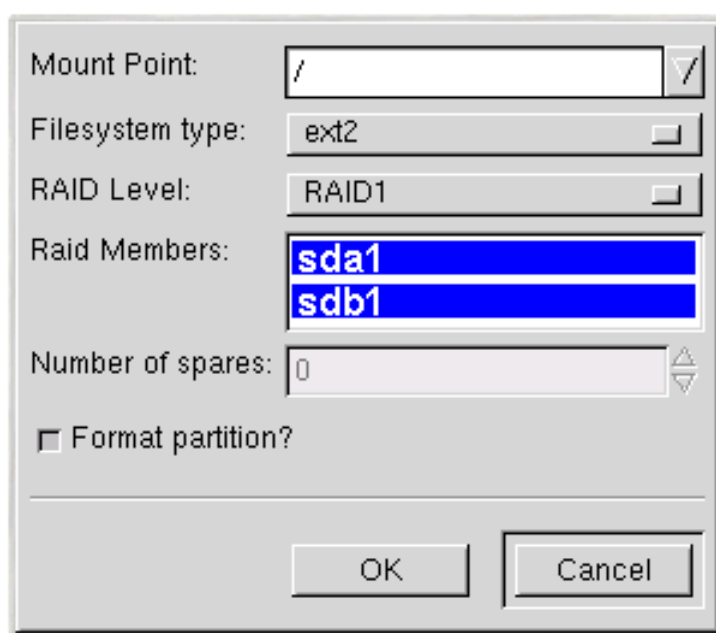


Abbildung 2-7: RAID Zusammenstellung

Diesen Dialog ruft man für jeden RAID Verbund erneut auf. Dabei wählt man den entsprechenden Mount Point, das Filesystem und die Mitglieder (Members) aus und bestätigt den Dialog. Die Zusammenstellung sieht nun so aus:

Tabelle 2-4: RAID Zusammensetzung

RAID Verbund	Partitionen
/dev/md0	/dev/sda4 + /dev/sdb4
/dev/md1	/dev/sda2 + /dev/sdb2
/dev/md2	/dev/sda3 + /dev/sdb3
/dev/md3	/dev/sda1 + /dev/sdb1

2.4 Bootloader

Nach der Partitionierung erscheint der Bildschirm für die Boot Konfiguration. Dabei können die Bootloader grub und lilo ausgewählt werden

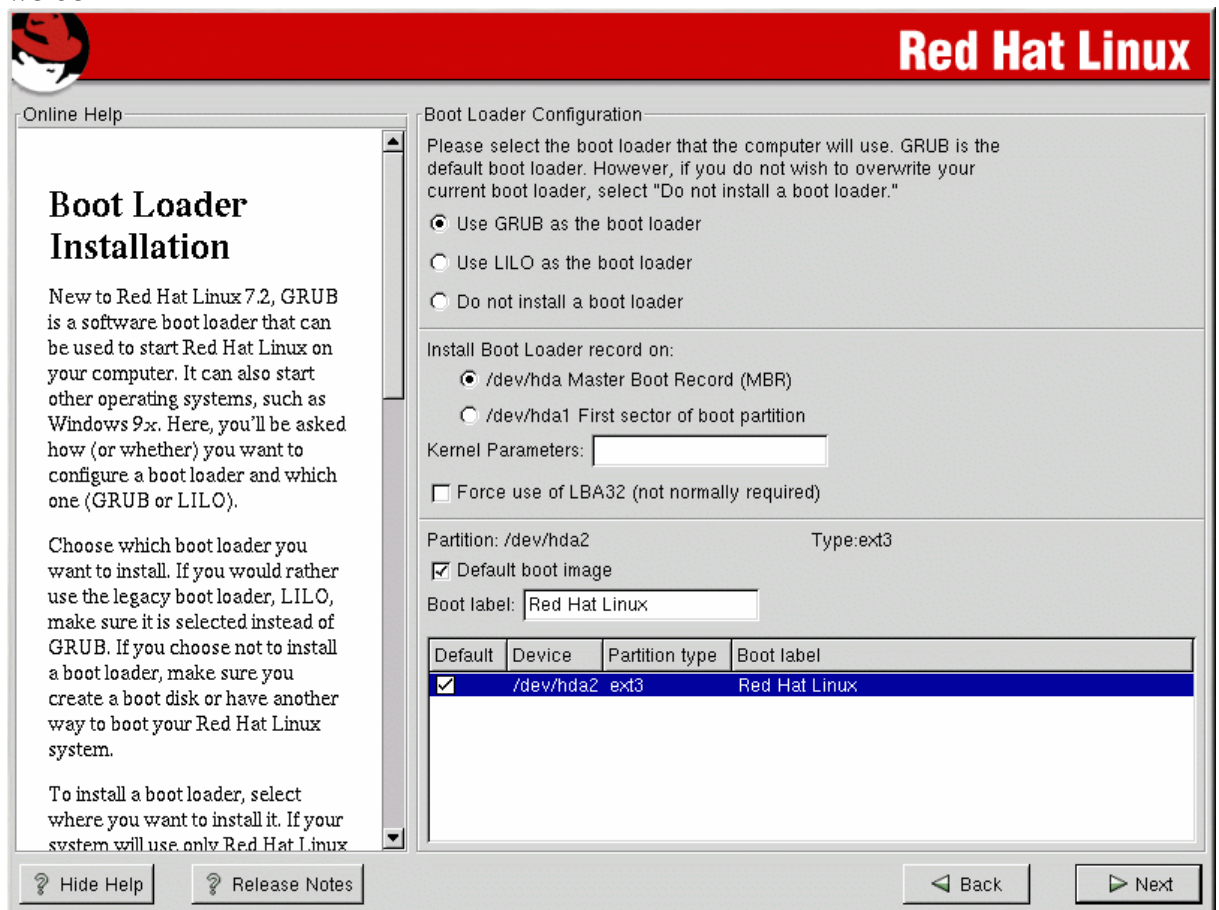


Abbildung 2-8: Bootloader

Wir haben den Linux Loader lilo auf dem Master Boot Record des RAID Verbundes md3 installiert.

2.5 Netzwerkkonfiguration

In diesem Dialog werden alle Angaben über die beim Start gefundenen Netzwerkkarten eingetragen.

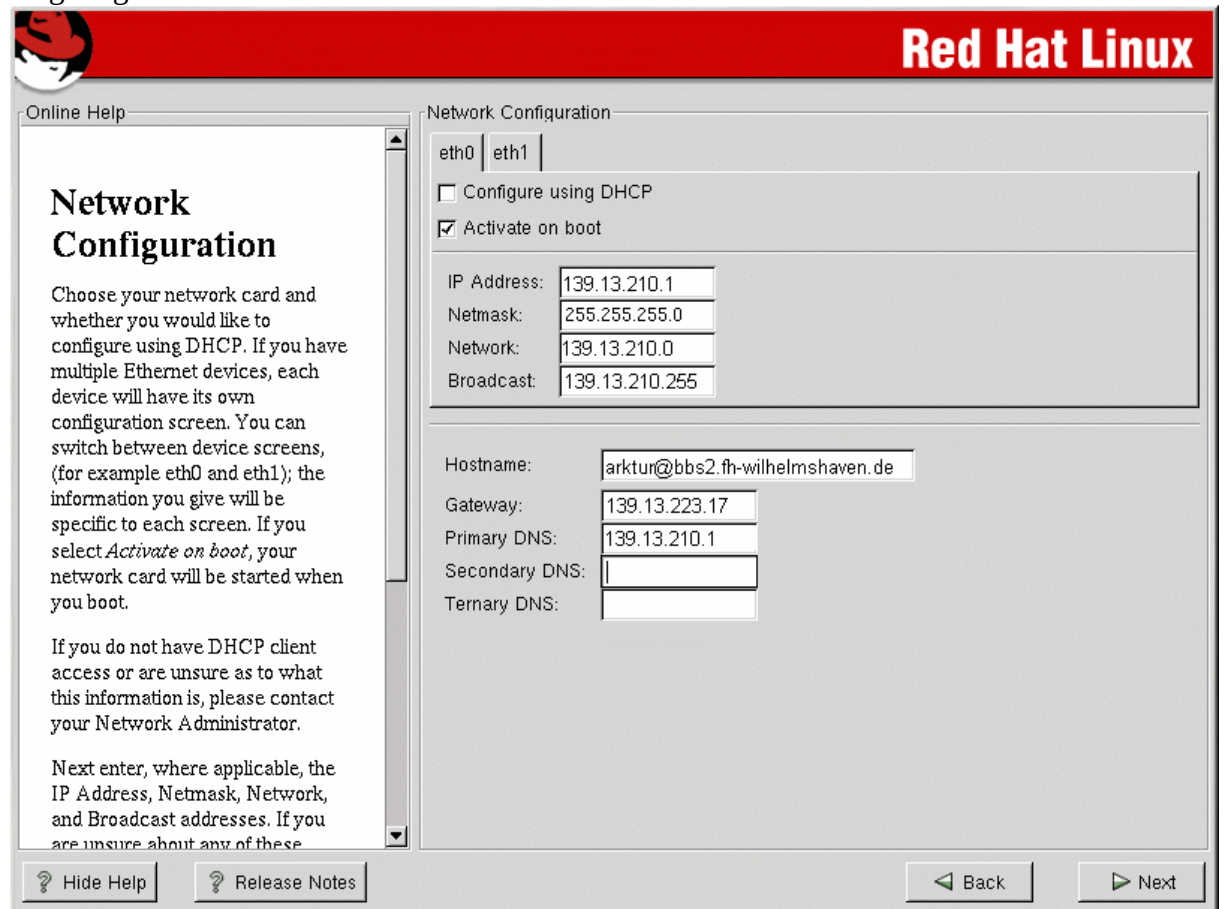


Abbildung 2-9: Netzwerkschnittstellen

In dem Server befinden sich 2 Interfaces. Dies sind die in den Reitern dargestellten eth0 und eth1. Dabei ist eth0 die Schnittstelle zur Fachhochschule und eth1 die Schnittstelle zum internen Schulnetz. Die folgende Tabelle beinhaltet alle nötigen Informationen zur Netzwerkkonfiguration.

Tabelle 2-5: Netzwerkdaten

	eth0	eth1
Netzwerkadresse	139.13.223.16	139.13.210.0
IP Adresse	139.13.223.18	139.13.210.1
Netzmaske	255.255.255.252	255.255.255.0
Broadcast	139.13.223.19	139.13.210.255
Primärer DNS	139.13.223.17	139.13.210.1
Gateway	139.13.223.17	139.13.223.17
Hostname	Arktur.bbs2.fh-wilhelmshaven.de	Arktur.bbs2.fh-wilhelmshaven.de

2.6 Firewall

Dieser Dialog gibt dem Benutzer die Möglichkeit eine einfache Firewall aufzusetzen. Da der Server allerdings eine erweiterte Firewall erhält, wird diese Funktion deaktiviert.

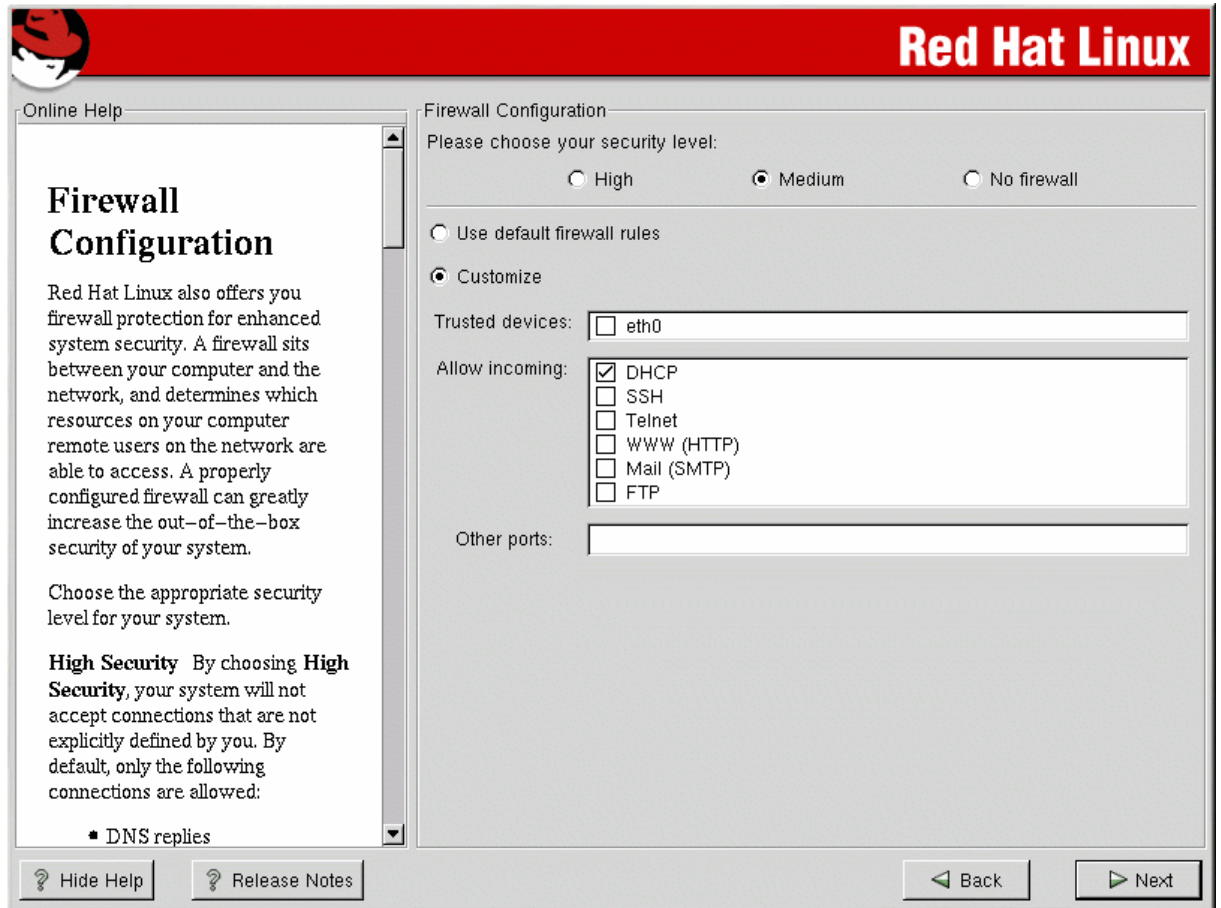


Abbildung 2-10: Firewallkonfiguration

2.7 Abschlusskonfiguration

Anschließend wird die Sprachunterstützung gewählt. Dabei werden unter anderem Wörterbücher für die gewählten Sprachen installiert. Sinnvollerweise wählt man hier mindestens Deutsch und Englisch (GB) aus.

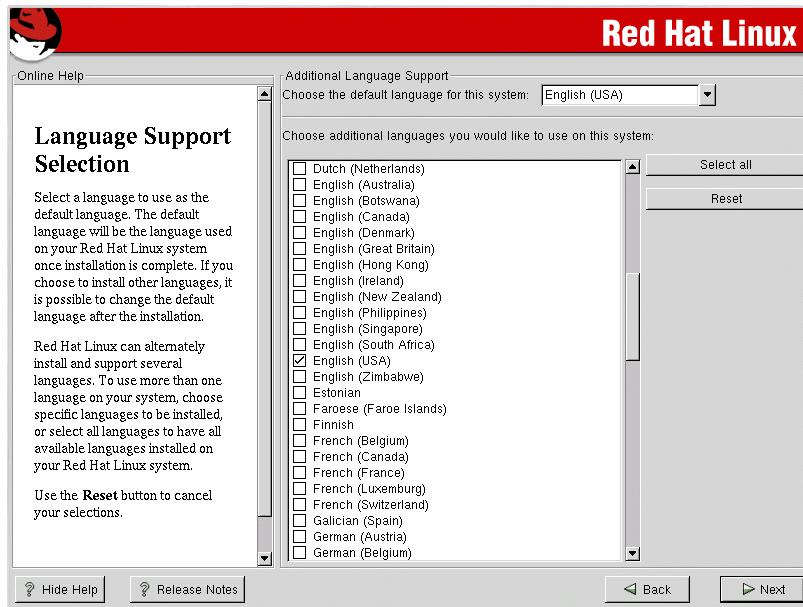


Abbildung 2-11: Sprachenunterstützung

Um die Uhrzeit und die lokale Zeitzone einzustellen dient der nächste Dialog. Der nächste Standort in der Liste ist Berlin.

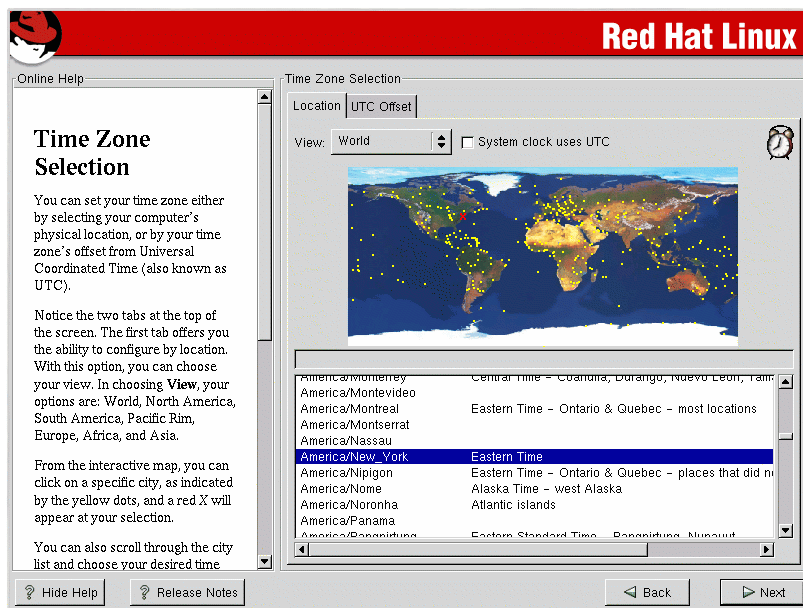


Abbildung 2-12: Zeitzone

2.8 Superuser – Passwort

Im folgenden Dialog wird nach dem Passwort für den Superuser gefragt. Weiterhin besteht hier die Möglichkeit weitere Benutzer anzulegen.



Abbildung 2-13: Superuser Passwort

Nach einem Klick auf Weiter kommt man zu den Authentisierungsoptionen. Dabei kann man die Standardeinstellungen ohne weiteres übernehmen.

2.9 Paketauswahl

Um zu bestimmen welche Software auf den Computer kopiert werden soll, gibt es nun die Möglichkeit einzelne Software Gruppen auszuwählen. Auf dem Server wurde eine Komplettinstallation vorgenommen. Diese belegt 2,3GB auf der Festplatte. Die dafür vorgesehene Option „everything“ steht ganz unten als letztes. Durch einen Haken in dem Feld „einzelne Pakete auswählen“ kann man die Zusammenstellung innerhalb der Software Gruppen beeinflussen.



Abbildung 2-14: Paketauswahl

Danach folgt die Auswahl der Grafikkarte. Hierbei wird meistens schon die richtige Karte vom System vorgeschlagen.

2.10 Kopieren

Jetzt beginnt das Installationsprogramm die Daten auf die Festplatte zu kopieren. Dabei wird der Verlauf für die Paketanzahl und die Zeit angezeigt.

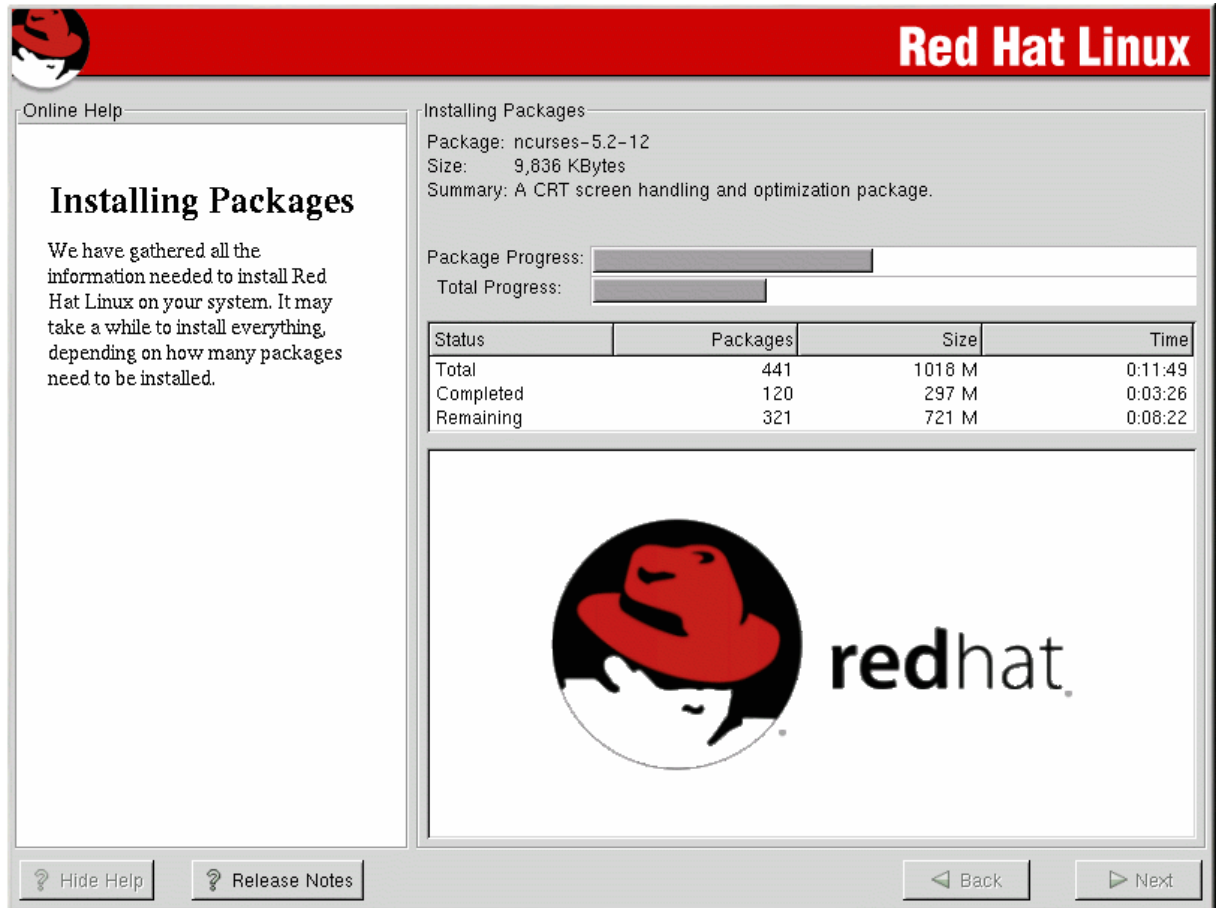


Abbildung 2-15: Kopiervorgang

Die letzten beiden Schritte der Installation sind nun das erstellen einer Bootdiskette für den Notfall und die Monitorauswahl.

Nach einem Neustart sollte man noch die Bootreihenfolge zurücksetzen damit in Zukunft direkt von der Festplatte gestartet werden kann.

Damit ist die Installation des Betriebssystems abgeschlossen.

3 Disk Quotas

3.1 Wozu Quotas gedacht sind

Um Festplattenplatz zu begrenzen setzt man Quotas ein. Damit kann man verhindern das Benutzer oder Gruppen Platz auf dem Server belegen der bekanntermaßen nicht wieder freigegeben wird. Es gibt dabei zwei unterschiedliche Arten: Hard und Soft Quotas:

Hard Quotas beschränken endgültig den benutzbaren Platz. Steht das Hard Limit auf 100MB kann der Benutzer auch nur über genau diese 100MB verfügen.

Soft Quotas ermöglichen dem Benutzer ein ausdehnen des benutzten Platzes bis hin zum Hard Limit und zwar für die Dauer der spezifizierten grace period (wörtlich: Gnaden-Zeit). Hat ein Benutzer also 75MB Soft und 100MB Hard Limit mit einer grace period von 3 Tagen, so kann er für 3 Tage an sein Hard Limit gehen und wird dann vom System aufgefordert die überbelegten 25MB wieder freizugeben.

Neben der Beschränkung des Platzes kann man auch die Anzahl der Dateien beschränken.

3.2 Vorbereitung zum Setzen der Quotas

Die Partitionen die mit Quotas beschränkt werden sollen erhalten in der Datei /etc/fstab bei den Mountoptionen den Zusatz usrquota für Benutzer bezogene Begrenzung beziehungsweise grpquota für eine Gruppenbegrenzung. Auch eine Kombination ist hier möglich.

Auszug aus der Filesystemtabelle des Arktur Servers:

/dev/md2	/home	ext2	defaults,usrquota	1	2
/dev/hdc1	/ide-platte/bbs-klassen	ext2	defaults,usrquota	1	2

Zu beachten war hierbei weiterhin, dass die bei der Installation automatisch mit Label versehene RAID Partition in ihren Gerätenamen (Device) umbenannt werden muss (hier von LABEL=/home in /dev/md2) da sich sonst die Quotas nicht aktivieren lassen.

Der nächste Schritt wäre laut Howto das Anlegen von zwei Dateien die den Platzverbrauch pro Benutzer beziehungsweise Gruppe speichern. Hier gibt es nun zwei Versionen:

```
aqouta.user und aquota.group
quota.user und quota.group
```

Diese Dateien sollten nur Lese- und Schreibrechte für root bekommen. Die Schritte würden so aussehen:

```
touch /partition/quota.user
touch /partition/quota.group
chmod 600 /partition/quota.user
```

```
chmod 600 /partition/quota.group
```

Es hat sich aber gezeigt dass diese Dateien bei der Quotaversion (quota-3.01pre9-3) von Red Hat 7.2 nicht benutzt werden, sondern die ersten beiden oben angeführten mit einem führenden a im Dateinamen. Diese wurde von dem Quotaprogramm beim aktivieren und überprüfen des Platzverbrauches selbst erzeugt. Die Rechte stehen dabei schon auf 600 (- rw- --- ---).

Der nächste Schritt ist, dem System die veränderten Filesystemeinstellungen mitzuteilen. Dazu montiert man die Partitionen ab und wieder an. In einigen Quellen ist von der Notwendigkeit die Rede das System komplett neu zu starten. Dies konnten wir aber nicht feststellen. Im Falle einer normalen Partition wie zum Beispiel /home kann man einfach folgende Schritte anwenden:

```
umount /dev/md2 /home  
mount /dev/md2 /home
```

Im Fall das auf der root Partition quotas verwendet werden, geht dies nicht, da das System nicht ohne Systemverzeichnis lauffähig ist. Hier muss man die Option `remount` benutzen:

```
mount /dev/md0 / -o remount
```

3.3 Aktivieren und editieren der Quotas

Um den aktuellen Platzverbrauch festzustellen ruft man zunächst das Programm `quotacheck` auf.

```
quotacheck -avug
```

dabei steht:

- a für alle montierten Filesysteme in `/etc/mtab`
- v für Fortschrittsanzeige
- u für Benutzerquotas und
- g für Gruppenquotas

Das editieren der einzelnen Begrenzungen erfolgt mit dem Programm `edquota`. Es benutzt dazu einen Systemeditor wie zum Beispiel `vi` (Standardeinstellung). Kommt man mit diesem nicht so gut klar oder will sich nicht umgewöhnen, kann man die Systemvariable `EDITOR` in der Datei `.bash_profile` aus dem eigenen Heimatverzeichnis exportieren. Sie sorgt dafür ein anderer Editor benutzt wird. In unserem Fall war dies `pico`:

```
export EDITOR=/usr/bin/pico
```

Damit diese Änderung wirksam wird, muss man sich ab- und wieder anmelden.

Nun kann man mit dem Aufruf

```
edquota -u USER1
```

die Begrenzungen für den Benutzer `USER1` ändern. Dazu gelangt man in den oben spezifizierten Editor `pico`. Dabei gilt gleiches für Gruppenquotas mit der Option `-g`. Im Editor erscheint jetzt folgende Übersicht

```
Diskquotas for User xyz (uid 4711)
Filesystem  blocks      soft      hard      inodes      soft      hard
/dev/md2    44          200000    200000    16           0         0
/dev/hdc1    0           0         0         0           0         0
```

dabei bedeuten in der zweiten Zeile der Reihenfolge nach:

```
blocks:      aktuell benutzte 1024k Blöcke
soft:        Softlimit für die Blöcke
hard:        Hardlimit für die Blöcke
```

```
inodes:      aktuelle Anzahl an Dateien
soft:        Softlimit für Dateianzahl
hard:        Hardlimit für Dateianzahl
```

Und dies für die jeweiligen Partitionen die in der ersten Spalte stehen. Eine 0 als Wert bedeutet dabei keine Beschränkung. Die Werte unterhalb von `block` und `inodes` sind, wie gezeigt, die aktuellen Werte. Sie sollten nicht editiert werden.

3.3.1 Einstellung der „Gnadenzeit“ (grace-period):

Mit dem Aufruf von `edquota` mit der Option `-t` gelangt man wieder in den Editor. Dieser zeigt folgendes Bild:

```
Time units may be: days, hours, minutes, or seconds
Grace period before enforcing soft limits for users:
Filesystem  block grace period    file grace period
/dev/md2:    7days                7days
/dev/hdc1:   7days                7days
```

Hier kann nun die Zeit einzeln für jede Partition und getrennt nach Softlimit für Platzverbrauch (`block`) und Dateianzahl (`file`) eingestellt werden. Die dabei möglichen Zeitdauervariablen stehen in der ersten Zeile.

3.3.2 Übertragen von Quotawerten auf mehrere Benutzer

Hat man sich einen Musterbenutzer erstellt so kann man mit der Option `-p` die Limits auf andere Benutzer (oder Gruppen) kopieren.

```
edquota -u MusterUser -p User1 User2 User3
```

Die vorhergehenden Vorgänge beziehen sich auf ein System das bereits aktive Benutzer hat und nun nachträglich der Festplattenplatz begrenzt werden soll. Hat man ein System zu dem man Benutzer erst noch hinzufügen muss, so kann man Standardwerte vorgeben die für jeden neuen Benutzer automatisch übernommen werden. Die Option verbirgt sich in der `Linuxconf` unter:

`Linuxconf` → Verwaltung → Benutzer → set quota defaults

3.3.3 Starten und beenden der Quotaüberwachung

Zum Starten und Beenden der Quotaüberwachung werden die Programme `quotaon` und `quotaoff` benötigt.

Mit

```
quotaon -avug
```

wird die Quotaüberwachung eingeschaltet, mit

```
quotaoff -avug
```

wird sie ausgeschaltet.

Dabei steht wieder:

`-a` für alle montierten Filesysteme in `/etc/mtab`

`-v` für Fortschrittsanzeige

`-u` für Benutzerquotas und

`-g` für Gruppenquotas

Der eingestellte Zustand bleibt dabei auch über einen Neustart hinaus erhalten.

Hinweis zu diesem Kapitel:

Die Einstellungen können auch alle mit Webmin vorgenommen werden, so wie es auch im Benutzerhandbuch steht. Dies funktionierte bei uns aber erst ab der Webmin Version 0.95. Diese Version erschien erst als die Quotas bereits fertig konfiguriert waren. Davor ließen sich die Quotas nicht aktivieren. Aus diesem Grund steht in dem vorhergehenden Kapitel die Vorgehensweise mit Hilfe der Konsole. In der Modulkonfiguration für Diskquotas unter Webmin finden sich all diese Befehle genauso wieder.

4 USV - Unterbrechungsfreie Stromversorgung

4.1 Die Aufgabe der USV

Server reagieren im allgemeinen sehr empfindlich auf Stromausfälle. Aufgrund ihrer Aufgabe viele verschiedene Dienste zur Verfügung zu stellen finden sehr viele Schreib- und Lesevorgänge statt. Linux hat mit dem Extended2 Filesystem die Eigenart die Daten nicht sofort auf die Festplatte zu schreiben, sondern verzögert in Blöcken. Fällt vor einem solchen Schreibvorgang der Strom aus, ist ein Datenverlust die Folge. Dies kann weitreichende Auswirkungen auf den Netzbetrieb haben. Denkbar wäre zum Beispiel das der DHCP Server den DNS Server updaten will, und das bei dem Schreibvorgang in die Zonendatei der Strom ausfällt. Eine zerstörte Zonendatei hindert den DNS Server daran die Namen für das LAN aufzulösen. In diesem Falle würde das Netzwerk stehen bis der Administrator eine neue Zone angelegt hat oder die hoffentlich vorhandene Sicherungskopie wieder eingespielt hat.

Um dies zu verhindern sichert eine unterbrechungsfreie Stromversorgung durch einen Pufferakkumulator die Stromversorgung ab. Sie befindet sich also zwischen Stromanschluss und Netzteil des zu schützenden Servers. Dabei überwacht sie ständig die anliegende Netzspannung. Sinkt diese unter einen voreingestellten Wert, schaltet die USV automatisch auf Batteriebetrieb.

Dies würde einen kurzen Stromausfall abfangen. Kurz hängt in diesem Fall von der Batteriekapazität ab. Die hier verwendet SmartUPS 1000 von APC hält den Server ungefähr eine dreiviertel Stunde oben. Damit dann der Server nicht doch noch kalt abgeschaltet wird, ist die USV mit einer seriellen Schnittstelle ausgerüstet. Über diese kann auf der einen Seite die USV konfiguriert werden und Statusvariablen abgefragt werden wie zum Beispiel Spannungen und Akkukapazität und auf der anderen Seite kann sie dem Server ein Signal geben, das der Strom ausgefallen ist, und ihn somit veranlassen, ordnungsgemäß herunterzufahren.

4.2 Installation der Hardware

Die Installation beginnt mit der Verbindung des Akkumulators mit der Ladeelektronik. Dieser ist hinter der Frontblende mit einem Hochstromstecker von der Elektronik getrennt. Auf dem Abdeckklebeband ist die Vorgehensweise illustriert. Danach verbindet man die serielle Schnittstelle mit einem freien COM Port an dem Server. Dabei ist zu beachten das es sich nicht um eine Standardleitung handelt. Es muss das mitgelieferte Kabel benutzt werden. Nachdem man dann den Server mit einem der mitgelieferten Kaltgeräteverlängerungskabel an die USV angeschlossen hat, kann man sie mit dem Stromnetz verbinden.

4.3 Installation der Software

Auf der mitgelieferten CD-ROM ist eine Konfigurationssoftware mit Namen PowerChute-Plus für die gängigsten Serverbetriebssysteme dabei. PowerChute liegt auf der CD im RPM Format vor. Dadurch ist die Installation sehr einfach. Nach dem einlegen und mounten der CD wird durch die Zeile

```
rpm -i /PFAD/ZUR/CD-ROM/PowerChutePlus-4.5.2.1-2.i386.rpm
```

das Paket eingespielt.

Danach befindet sich das Programm komplett im Verzeichnis

```
/usr/lib/powerchute/
```

4.4 Konfiguration

Die Konfiguration erfolgt zunächst durch ein Konfigurationsskript das sich im Programmverzeichnis befindet. Die Aufrufe

```
cd /usr/lib/powerchute/  
./Config.sh
```

starten das Skript.

```
[root@arktur powerchute]# ./Config.sh  
-----  
PowerChute Plus for Linux v4.5.3 Configuration Script  
Copyright American Power Conversion 2001  
-----  
  
1) Matrix-UPS  
2) Smart-UPS  
3) Back-UPS  
4) Back-UPS Pro  
5) Symmetra Power Array  
6) Smart-UPS DP
```

```
Which APC Hardware will PowerChute Plus for UNIX be running with [?] 2
```

Die erste Abfrage richtet sich auf die verwendete Hardware. Bei uns war es eine SmartUPS 1000. Danach fragt das Skript eine Optionale Messerweiterung vorhanden ist. Dies war nicht der Fall:

```
-----  
The Measure-UPS is a device which is designed to perform environmental  
monitoring in conjunction with PowerChute Plus for UNIX  
-----
```

```
Do you currently have a Measure-UPS attached to the UPS? [y/n] n
```

Die folgende Frage bezieht sich auf die Möglichkeit andere Computer über TCP/IP Netzwerke zu überwachen. Da keine anderen Computer überwacht werden sollen und ein Fehler beim Aufrufen des Programms auftrat der besagte das keine Verbindung zum Server aufgenommen werden kann haben wir diese Frage verneint. Somit läuft der Prozess nur Lokal.

```
-----  
PowerChute Plus for UNIX is able to monitor other hosts. However, in order  
to monitor other hosts TCP/IP must be installed. If you do not have  
TCP/IP installed, answer 'n' to the following question.  
-----
```

```
Do you currently have TCP/IP Installed? [y/n] n
```

Da PowerChute-Plus unter Red Hat 7.2 nur auf der grafischen Oberfläche lauffähig ist, spielt die Antwort auf die Frage nach dem Farbschema keine Rolle. Sie ist für Versionen die auf der Textkonsole laufen gedacht.

```
-----
If you will be using the Motif version of the User Interface on a
monochrome monitor, using the Monochrome Coloring scheme is recommended.
-----
```

- ```
1) Use Default Color scheme
2) Use Monochrome Color scheme
```

```
Which color scheme do you wish to use [1]? 1
```

Die serielle Schnittstelle die verwendet werden soll wird in dem folgenden Dialog spezifiziert. Dabei steht ttyS0 für COM Port 1 und ttyS1 für COM Port 2. Unter Other kann ein anderer konfiguriert werden.

```

PowerChute Plus for UNIX requires complete control of the serial port. No
processes, including gettys, are allowed to be accessing the port.
Therefore, the serial port you select must NOT be enabled for logins. To
ensure that PowerChute Plus for UNIX has control of the serial port, make
sure that it is not enabled for logins. To disable the port for logins
consult the PowerChute Plus for UNIX manual.

```

- ```
1) /dev/ttyS0
2) /dev/ttyS1
3) Other
```

```
Which serial device will be dedicated to PowerChute Plus for UNIX [?] 1
```

Nun wird man aufgefordert sich zu vergewissern das das Spezialkabel mit der UPS und dem Rechner verbunden ist.

```
-----
You should have the black cable, #940-0024C attached to /dev/ttyS0
Please verify.
-----
```

```
-----
Command files may be executed with root privileges or with the
privileges you assign to the pwrchute account (allowing you to
customize command file execution according to your system
requirements).
-----
```

```
Do you want to execute command files as root? [y/n] y
```

```
-----
E-mail may be sent with root privileges or with the privileges you
assign to the pwrchute account.
-----
```

```
Do you want to send e-mail as root? [y/n] n
```

Diese zwei Fragen beziehen sich auf das Verhalten das PowerChute an den Tag legt wenn es Befehle ausführt und Emails verschickt. Man kann wählen ob diese Aktionen als Benutzer powerchute oder als Superuser ausgeführt werden sollen.

Zum Schluss zeigt das Skript eine Zusammenfassung an und schließt mit einer Sicherheitsabfrage ab.

```
-----  
PRODUCT                : PowerChute Plus for UNIX  
DEDICATED TTY           : /dev/ttyS0  
UPS TYPE                : Smart-UPS  
Measure-UPS INSTALLED  : FALSE  
INSTALLING AS ROOT     : TRUE  
TCP/IP Installed       : FALSE  
RUN COMMAND FILES AS ROOT : TRUE  
SEND EMAIL AS ROOT     : FALSE  
-----
```

Are the above selections correct? [y/n]

5 DNS – Der Domain Name Service

5.1 Warum der DNS Server ein Telefonbuch ist.

Der Domain Name Service stellt im Internet so etwas wie eine Auskunft dar die von einem anfragenden Client eine Internet Adresse in eine gültige IP Adresse übersetzt. Der DNS Server legt zu diesem Zweck eine so genannte Zonen Datei an in der die IP Adressen und die dazu gehörigen Host Namen wie in einer Tabelle nebeneinander stehen. Dieser Vorgang ist eine so genannte forward oder Vorwärts-Auflösung. Um einen Domänen Namen zu einer vorhandenen IP Adresse zu finden gibt es die revers oder Rückwärts-Auflösung. Dies ist allerdings nicht immer von den Domäneninhabern erwünscht und für einige daher deaktiviert. Die Vorwärts-Auflösung ist aber dennoch möglich. Für diese so genannte reverse Anfrage wird auch eine Zonen Datei erzeugt. Die beiden Zonen Dateien liegen im Verzeichnis

```
/var/named/
```

Sinnvollerweise benennt man die Zonen Dateien nach dem Schema *named.domain* und *named.domain-rev*.

5.2 Installation und Konfiguration

Der DNS Dämon *named* (bind9) ist nach der Vollinstallation von Red Hat Linux 7.2 mit installiert. In seiner Grundeinstellung startet er allerdings nicht automatisch. Um dies sicherzustellen kann man entweder per Hand die Verknüpfungen zu dem Startscript für die einzelnen Runlevel erzeugen oder komfortabel über das Tool *Linuxconf* einschalten.

Linuxconf → System → Kontrolltafel → Dienste → named

Die Konfiguration erfolgt in der Datei */etc/named.conf*

Auszug:

```
zone "bbs2.fh-wilhelmshaven.de" {
    type master;
    file "/var/named/named.BBS2";
    allow-update { key DHCP_UPDATER; };
};

zone "210.13.139.in-addr.arpa" {
    type master;
    file "/var/named/named.BBS2-rev";
    allow-update { key DHCP_UPDATER; };
};
```

Für die Domäne *bbs2.fh-wilhelmshaven.de* wurden hier 2 Zonen angelegt. Die erste für die Vorwärts-Auflösung, die zweite für die Rückwärts-Auflösung. Dazu werden jeweils die Dateinamen mit Pfaden angegeben. Der Eintrag *allow-update* ermöglicht es einem anderen Programm das über den Schlüssel (*key*) mit dem Namen *DHCP_UPDATER* verfügt die Zonendatei zu verändern. In unserem Fall soll der DHCP Server die IP Adresse und den Hostnamen die er vergeben hat in die Zonen eintragen. Um dies abzusichern wird ein Schlüssel benutzt den man mit dem Keygenerator (*dnssec-*

keygen) des DNS Paketes erzeugen kann. Diesen trägt man dann in der `secret` Anweisung im `key` Bereich ein:

```
key DHCP_UPDATER {  
    algorithm HMAC-MD5.SIG-ALG.REG.INT;  
    secret xxxxxxxxxxxxxxxxxxxxxxxxx;  
};
```

Aus Sicherheitsgründen ist der `key` hier unkenntlich gemacht worden. Der Keygenerator erzeugt eine Datei in der der Schlüssel im Klartext steht. Diesen kann man kopieren und in die `secret` Anweisung einfügen.

Der Eintrag `algorithm` spezifiziert den benutzten Verschlüsselungsalgorithmus. Weitere Informationen zu den möglichen Verschlüsselungen gibt es in den Handbuchseiten von `dhcpcd.conf` und `dnssec-keygen`.

6 DHCP – Dynamische IP Adressenvergabe

6.1 Installation

Die DHCP Version die mit der Red Hat Distribution geliefert wird ist nicht dazu geeignet den DNS Server dynamisch aufzufrischen. Es existiert die Möglichkeit dies mit selbst geschriebenen Skripten zu tun, jedoch bietet die zum Projektbeginn erschienene Version 3 des DHCP Paketes diese Funktion. Darum war ein Update notwendig.

6.2 Konfiguration

Die Konfiguration erfolgt in der Datei `/etc/dhcpd.conf`.

```
#ddns-update-style ad-hoc;
ddns-update-style interim;
# dhcpd.conf
#
# Configuration file for ISC dhcpd
server-identifier server.bbs2.fh-wilhelmshaven.de;
#server-identifier 139.13.210.1;

# Der Domain-Name
option domain-name "bbs2.fh-wilhelmshaven.de";

# Der (die) Domain Nameserver

option domain-name-servers 139.13.210.1;
#option netbios-name-servers 139.13.210.1;

# Der default Router
option routers 139.13.210.1;

# Die Subnetzmaske
option subnet-mask 255.255.255.0;

# 1 Tag Zuteilungsdauer fuer eine IP-Nummer
default-lease-time 86400;

# 5mal soviele als Maximum
max-lease-time 432000;

key DHCP_UPDATER {
    algorithm HMAC-MD5.SIG-ALG.REG.INT;
    secret xxxxxxxxxxxxxxxxxxxxxxxxxxxxx;
}

zone BBS2.FH-WILHELMSHAVEN.DE {
    primary 127.0.0.1;
    key DHCP_UPDATER;
}

zone 210.13.139.in-addr.arpa. {
    primary 127.0.0.1;
    key DHCP_UPDATER;
}

subnet 139.13.210.0 netmask 255.255.255.0 {
    range 139.13.210.222 139.13.210.254;
    option broadcast-address 139.13.210.255;
}
```

6.2.1 Erklärung der Direktiven:

ddns-update-style:

Diese Zeile gibt die Methode für das dynamische DNS Update vor. Zum Zeitpunkt der Drucklegung sind zwei Update Typen verfügbar: der ad-hoc und der interim Style. Interim bedeutet soviel wie Übergang oder zwischenzeitlich und meint das bis zur Verabschiedung der dritten, angestrebten Version diese als aktuell gilt. Weiterhin ist davon die Rede das sich die endgültige nicht viel von der jetzigen Interim Methode unterscheiden wird. Der ad-hoc Style wird als nicht funktionsfähig bezeichnet. Nachzulesen in der Handbuchseite von dhcpd.conf.

ACHTUNG: Vor allem bei der ad-hoc Methode ist uns einige Male der DNS Server stehen geblieben. Der Grund dafür ist das die Vergaben nicht sofort in die Zonen Dateien geschrieben werden, sondern vorerst im RAM und in den nicht lesbaren Journal Dateien festgehalten werden. Das hat den Sinn, das der Server in einer Firma oder Schule bei Arbeitsbeginn oder Ende für durchaus mehrere Hundert an- oder abmeldende Rechner einzelne Schreibvorgänge auf die Zonen Datei ausführen müsste. Sollte dies der Fall sein braucht man nur die Journal Dateien zu löschen und den DNS und DHCP Server neu zu starten. Sie befinden sich in dem Ordner wo sich auch die Zonen Dateien befinden.

/var/named/

Die Dateien heißen genau wie die jeweiligen Zonen und haben die Endung .jnl. Bei der Umstellung auf den interim Style konnten wir nur noch gelegentliche Abstürze beobachten. Es kann daher davon ausgegangen werden das bei der noch erscheinenden dritten Methode diese Abstürze nicht mehr auftreten werden. Wir raten deshalb dazu ein Update einzuspielen sobald dies verfügbar ist und die Update Methode in der dhcpd.conf umzuändern.

server-identifizier:

Diese Zeile gibt dem Server einen Namen

option domain-name:

Hier wird dem Server die Domäne mitgeteilt für die er zuständig ist.

option domain-name-servers:

Festlegung des für die Domäne zuständigen DNS Servers.

option routers 139.13.210.1;

Angabe über den Router über den die Vergaben geleitet werden.

option subnet-mask 255.255.255.0;

Netzmaske des Unternetzes.

default-lease-time 86400;

Standard Vergabe Zeit in Sekunden. (Hier: 1 Tag)

max-lease-time 432000;

Maximale Vergabe Zeit in Sekunden. (Hier 5 Tage)

key DHCP_UPDATER:

Festlegung des für den Updateprozess vereinbarten Sicherheitsschlüssel. Nur bei Verwendung dieses Schlüssels erlaubt der DNS Server ein Update. Siehe dazu auch Abschnitt 5.2.

zone BBS2.FH-WILHELMSHAVEN.DE:

Angabe über die Zone für die Vorwärtsauflösung.

zone 210.13.139.in-addr.arpa.:

Angabe über die Zone für die Rückwärtsauflösung.

**subnet 139.13.210.0 netmask 255.255.255.0 {
 range 139.13.210.222 139.13.210.254;
 option broadcast-address 139.13.210.255;
}**

Hier wird der Bereich für die Adressenvergabe eingegrenzt und die Broadcast Adresse festgelegt.

7 Apache – Der Internet Server

7.1 Aufgabe des Servers

Apache ist der weit verbreitetste Internetserver auf dem Globus. Er stellt auf Anfrage eines Clients HTML Dokumente zur Verfügung. Sein Erfolg basiert wohl auf der großen Flexibilität und Plattformunabhängigkeit. So kann ein Apache Server Internetseiten für mehrere Domänen verwalten und nebenbei auch noch als Proxy für ein lokales Netz dienen.

Apache besteht aus mehreren Modulen die während der Laufzeit dynamisch nachgeladen werden können.

7.2 Installation und Konfiguration

Der Apache Webserver wird mit der Vollinstallation von Red Hat 7.2 mit installiert. Seine Konfiguration geschieht in der Datei `/etc/httpd/conf/httpd.conf`. Dies kann manuell in einem beliebigen Editor erfolgen oder mit Hilfe eines der vielen Konfigurationstools. In Red Hat 7.2 ist beispielsweise `apacheconf` enthalten. Weiterhin gibt es `Comanche` oder das hier verwendete `Webmin`.

7.3 Aufgaben

Als erstes soll der zu erstellende Server die Internet Seiten der BBS II der Außenwelt zur Verfügung stellen. Die Zweite Aufgabe ist eine Plattform für Unterrichts- und Versuchszwecke zur Verfügung zu stellen. Auf dieser können die Schüler selbst erstellte HTML Dokumente unter realen Bedingungen testen. Die dritte Aufgabe sieht vor, das alle vom lokalen Netz aus aufgerufenen Internetseiten durch einen Stellvertreter (Proxy) angefordert werden.

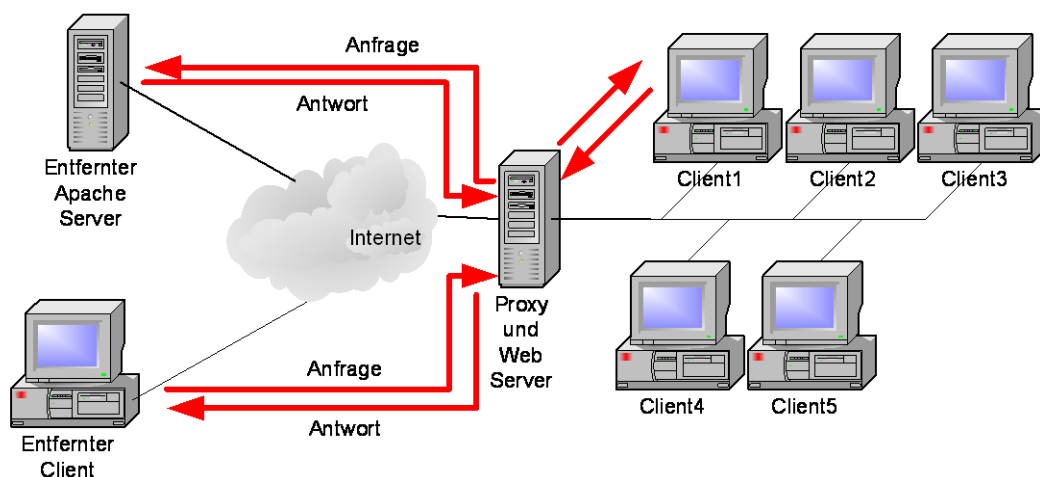


Abbildung 7-1: Proxyprinzip

7.4 Bemerkungen über das Proxy Modul

Bei der Konfiguration per Webmin traten mit dem Proxymodul einige Schwierigkeiten auf. Dazu gehört das sich das Modul nicht über die Modulkonfiguration einschalten ließ.

Um den Proxy Modus einschalten zu können müssen in der httpd.conf die Kommentarzeichen vor den folgenden Zeilen entfernt werden:

```
#LoadModule proxy_module          modules/libproxy.so
```

und

```
#AddModule mod_proxy.c
```

Weiterhin bemängelte Webmin die Proxydomänendirektiven als “invalid” also ungültig und brach den Speichervorgang ab. Trägt man diese Direktiven manuell in die httpd.conf ein und startet den Apache funktioniert alles wie vorgesehen. Da wir ein ähnliches Problem mit den Disk Quotas hatten, welches durch eine neuere Version von Webmin behoben wurde, raten wir dazu die Webmin Versionen zu beobachten und bei Behebung dieses Fehlers ein Update einzuspielen. Im Gegenwärtigen Zustand ist die Webminseite über die Proxy Einstellungen nur zur Übersicht zu gebrauchen.

[Webmin Index](#)
[Modul Index](#)

Proxying

[Änderungen zuweisen](#)
[Apache beenden](#)

Für www.bbs2.fh-wilhelmshaven.de:8080

Proxying für www.bbs2.fh-wilhelmshaven.de:8080

Act as proxy server?
☒ Ja
☐ Nein

Cache directory
☐ None
☒ "/ide-platte/proxy-cache"

Block requests to domains
☐ None
☒ sex playboy eroti xxx blow happy night climax edda teens and

Requests to pass to another proxy

Requests

Forward to

☒ All
☐ Matching

Don't pass requests to another proxy for

Type

No proxy for..

Domain
 bbs2.fh-wilhelmshaven.de

IP address

Domain for requests with no domain
☐ None
☒ bbs2.fh-wilhelmshaven.d

Domains not to cache
☐ None
☒ bbs2.fh-wilhelmshaven.d

Ports to which CONNECT is allowed
☒ Default
☐

Cache default expiry time
☐ Default
☒ 6 hours

Cache directory name length
☒ Default
☐

Cache directory levels
☒ Default
☐

Finish and cache transfer after
☒ Default
☐ %

Cache garbage collection interval
☐ Never
☒ 10 hours

Cached file expiry time factor
☐ Default
☒ 0.7

Cached file maximum expiry time
☐ Default
☒ 120 hours

Cache size
☐ Default
☒ 3500000 kB

Speichern

Abbildung 7-2: Proxyeinstellungen eines Virtuellen Servers

7.5 Die virtuellen Server

Damit der Server die Aufgaben bedienen kann wird er in 3 virtuelle Server Aufgeteilt. Der erste kümmert sich um Anfragen von außen, der zweite um Anfragen von innen und der dritte ist der Testserver für Schüler. Dabei übernimmt der zweite gleichzeitig die Aufgabe der Zwischenspeicherung (Proxy).

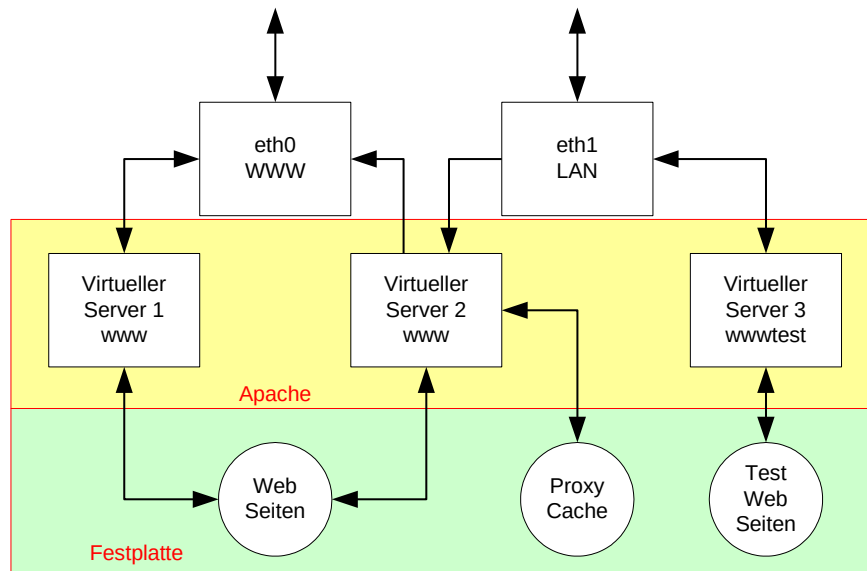


Abbildung 7-3: Virtuelle Server

7.5.1 Anlegen eines virtuellen Servers

Um einen virtuellen Server zu erstellen kann man die Eingabemaske am unteren Rand der Apache Startseite benutzen. Dabei bedeuten die Felder folgendes:

Adresse:

Hier kann sowohl die IP Adresse als auch der Hostname eingetragen werden. Bei einem Hostnamen muss allerdings beachtet werden das Apache bei jedem Start eine DNS Abfrage sendet. Erhält er keine Antwort, startet der virtuelle Server nicht.

Add Name Virtual Host:

Soll der neue Server ein Namensbasierter Virtueller Host sein und die dafür nötige Direktive NameVirtualHost on ist nicht in der httpd.conf vorhanden, wird sie hinzugefügt. (if needed)

Anschluss:

Port Nummer auf die der Server hören soll.

Document Root:

Verzeichnis das die HTML Dateien enthält.

Server Name:

Name unter dem der Server angesprochen wird. (z.B.: www)

Copy directives from:

Hier kann ein Profil eines anderen Servers geklont werden.

Nach einem Klick auf <ERSTELLEN> werden die Einstellung in der httpd.conf gespeichert. Um den neuen Server in der Liste sehen zu können, muss die Seite aktualisiert werden.

[Webmin Index](#)
[Modul-Konfiguration](#)

Apache-Webserver

[Änderungen zuweisen](#)
[Apache beenden](#)
[Suche in der Hilfe](#)

Globale Konfiguration

 Prozesse und Grenzwerte	 Netzwerk und Adressen	 Apache-Module	 MIME-Typen	 Verschiedenes
 CGI-Programme	 Per-Verzeichniseinstellungsdateien	 Bekannte Module neu konfigurieren	 Definierte Parameter bearbeiten	 Edit Config Files

Virtuelle Server

Typ	Adresse	Anschluss	Server-Name	Dokumenten-Root
Standard-Server	Beliebig	Beliebig	www.bbs2.fh-wilhelmshaven.de	Automatisch
Virtueller Server	139.13.210.180 139.13.210.18080	80	www.bbs2.fh-wilhelmshaven.de	/var/www/bbs2
Virtueller Server	139.13.223.18	80	www.bbs2.fh-wilhelmshaven.de	/var/www/bbs2
Virtueller Server	139.13.210.1	80	wwwtest.bbs2.fh-wilhelmshaven.de	/var/www/wwwtest

Einen neuen virtuellen Server anlegen

Adresse ☐ Beliebig ☐

☒ Add name virtual server address (if needed)

Anschluss ☐ Standard ☐ Beliebig

Dokumenten-Root

Server-Name ☐ Automatisch ☐

Copy directives from

[← Zurück zu Startseite](#)

Abbildung 7-4: Apache Startseite

Nun kann man durch anklicken eines Links in der Liste der virtuellen Server die Einstellungen für jeden einzelnen Server anpassen.

Wie in der Liste zu sehen ist, greifen die Virtuellen Server mit dem Namen www auf das Dokumentenverzeichnis /var/www/bbs2 zu. In diesem befinden sich die Internetseiten der BBS II. Der Dritte Server der auf wwwtest hört greift dagegen auf /var/www/wwwtest zu. Diese Verzeichnis ist gleichzeitig eine Samba Fileserver Share. Dies bedeutet das Schüler über den Windows Explorer von einem Schulrechner aus ihre selbst erstellten Webseiten in das Dokumentenverzeichnis von wwwtest legen können. Somit ist ein sofortiges testen der Seiten im LAN möglich. Im LAN deshalb, weil der wwwtest nur auf die Schul interne Schnittstelle hört.

8 wu-ftp – Der FTP Server

8.1 Installation und Start von wu-ftp

Der verwendete wu-ftp Server wird bereits mit der Vollinstallation mit installiert. Das Startverhalten wird über den Extended Internet Superserver xinetd gesteuert. Dazu ist für jeden seiner Dienste eine Textdatei im Verzeichnis `/etc/xinetd.d/` vorhanden. Im Falle des wu-ftp ist dies:

`/etc/xinetd.d/wu-ftp`

In dieser Datei steht auch das auszuführende Programm (`/usr/sbin/in.ftpd`). Um den Server mit dem xinetd zu starten muss die Zeile `disable = yes` in `disable = no` abgeändert werden.

Alternativ kann man in Webmin unter dem Registerreiter Server und dann dem Eintrag Extended Internet Services den Service FTP auswählen und bearbeiten.

[Webmin Index](#)
[Modul Index](#)

Edit Internet Service

Service network options			
Service name	ftp	Service enabled?	☒ Ja ☐ Nein
Bind to address	☒ All ☐	Port number	☒ Standard ☐
Socket type	Stream	Protocol	Default

Service program options			
Service handled by			
☐ Internal to Xinetd ☒ Server program /usr/sbin/in.ftpd -l -a ☐ Redirect to host port			
Run as user	root	Run as group	☒ From user ☐
Wait until complete?	☐ Ja ☒ Nein	Max concurrent servers	☒ Unlimited ☐
Nice level for server	☐ Default ☒ 10	Maximum connections per second	☒ Unlimited ☐
		Delay if maximum is reached	seconds

Service access control	
Allow access from	Deny access from
☒ All hosts ☐ Only listed hosts.. 	☒ No hosts ☐ Only listed hosts..
Allow access at times	
☒ Any time ☐	

← [Zurück zu service list](#)

Abbildung 8-1: FTP Dienst aktivieren

Nach einem Neustart des Superservers ist wu-ftp aktiv. Dazu gibt man auf der Konsole folgendes ein:

```
/etc/init.d/xinetd restart
```

Um die Server beim booten zu aktivieren, muss xinetd als Startdienst eingetragen sein. Dies kann wieder manuell über Links in den Runlevel Verzeichnissen, über Linuxconf oder Webmin erledigt werden.

Weiterhin muss noch eine geeignete Verzeichnisstruktur für den FTP Server erstellt werden. Bei der gegebenen Hardware wurde eigens für den FTP Server eine 2 GB Partition angelegt die an den Mount Point `/ide-platte/ftp` angehängt wurde. Darunter wurden Verzeichnisse für FTP typische Art angelegt. Dies sind zum einen ein `public` Verzeichnis und zum anderen ein `incoming` Verzeichnis zum Hochladen. Denkbar wäre hier auch ein Link zum `wwwtest` Ordner um von außen HTML Seiten zum testen in das Dokumentenverzeichnis des Apache zu laden. Dies dürfte allerdings nicht für anonyme Benutzer erlaubt sein.

8.2 Konfiguration

8.2.1 Verzeichnisse

Die Grundlegenden Einstellungen sind zunächst die Angaben über die Verzeichnisse. Dazu klickt man unter Webmin (über Server → wu-ftp) auf das Icon Aliases und Pfade.

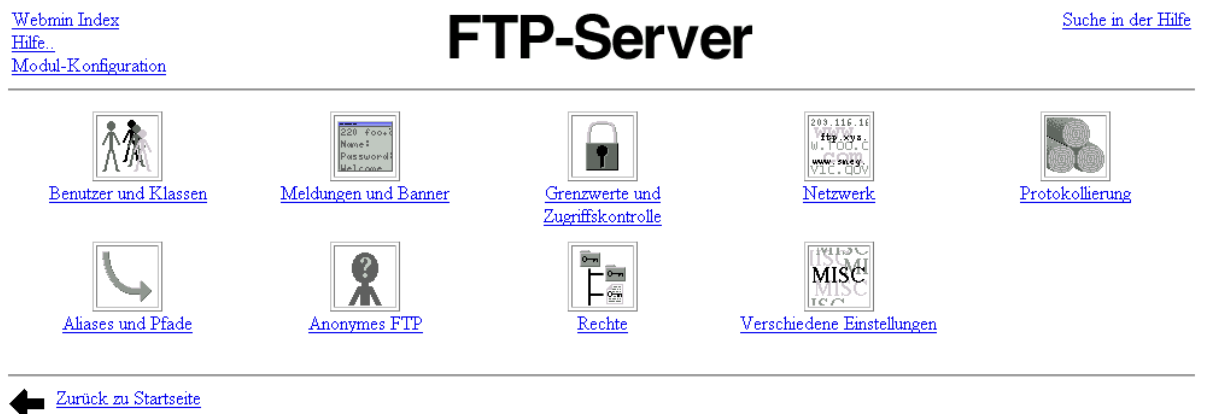


Abbildung 8-2: FTP Startseite

[Webmin Index](#)
[Modul Index](#)
[Hilfe](#)

Aliases und Pfade

Alias- und Pfadeinstellungen

CD-Verzeichnis-Aliases

Alias-Name	Alias zu Verzeichnis
pub	/ide-platte/ftp/public
incoming	/ide-platte/ftp/incoming
cdrom	/ide-platte/ftp/cdrom

CD-Verzeichnissuchpfad

Speichern

← [Zurück zu FTP-Server-Einstellungen](#)

Abbildung 8-3: Aliases und Pfade

Hier werden die Namen erzeugt die ein Benutzer statt der richtigen Verzeichnisnamen zu sehen bekommt. Es können statt Verzeichnisse auch Links angegeben werden. Im Bild oben ist `/ide-platte/ftp/cdrom` ein Softlink auf `/mnt/cdrom`.

8.2.2 Anonymes FTP

Um unbekannten Benutzern den Zugang zum FTP Server zu gestatten wird ein so anonymer Zugang eingerichtet. Zu diesem Zweck bekommt er quasi ein eigenes Heimatverzeichnis `/ide-platte/ftp`. Eingestellt werden diese Optionen unter Anonymes FTP auf der Hauptseite von wu-ftp.

[Webmin Index](#)
[Modul Index](#)
[Hilfe](#)

Anonymes FTP

Einstellungen für anonymes FTP			
Root-Verzeichnis für anonymes FTP		Verzeichnis	Für Klasse
		/ide-platte/ftp	Beliebig
			Beliebig
Gast-Root-Verzeichnis		Verzeichnis	Für Unix-Benutzer
		/ide-platte/ftp	/ide-platte/ftp
Unix-Gruppen für anonyme Benutzer		Wechsle zu Gruppe	Für Klassen
			☐ all
Kennwortüberprüfung für anonymes FTP		☐ Default ☒ Muss eine E-Mail-Adresse nach RFC822 sein	
Kennwörter für anonymes FTP, die verweigert werden sollen			
Speichern			

← [Zurück zu FTP-Server-Einstellungen](#)

← [Zurück zu FTP-Server-Einstellungen](#)

Abbildung 8-4: Anonymes FTP

8.2.3 Benutzer und Klassen

Um einzustellen welche Benutzer und Klassen welche Rechte bekommen sollen, klickt man auf der Server Hauptseite auf Benutzer und Klassen:

[Webmin Index](#)
[Modul Index](#)
[Hilfe](#)

Benutzer und Klassen

Benutzerklassen und Benutzereinstellungen											
Benutzerklassen	<table border="1"> <thead> <tr> <th>Klassenname</th> <th>Benutzertypen</th> <th>Übereinstimmende Adressen</th> </tr> </thead> <tbody> <tr> <td>all</td> <td>☒ Unix ☒ Anonym ☒ Gast</td> <td>*</td> </tr> <tr> <td></td> <td>☐ Unix ☐ Anonym ☐ Gast</td> <td></td> </tr> </tbody> </table>	Klassenname	Benutzertypen	Übereinstimmende Adressen	all	☒ Unix ☒ Anonym ☒ Gast	*		☐ Unix ☐ Anonym ☐ Gast		
Klassenname	Benutzertypen	Übereinstimmende Adressen									
all	☒ Unix ☒ Anonym ☒ Gast	*									
	☐ Unix ☐ Anonym ☐ Gast										
Unix-Benutzer und UIDs, die als Gäste behandelt werden sollen											
Unix-Gruppen und GIDs, die als Gäste behandelt werden sollen	ftpchroot										
Unix-Benutzer und UIDs, die <i>nicht</i> als Gäste behandelt werden sollen											
Unix-Gruppen und GIDs, die <i>nicht als Gäste behandelt werden sollen</i>											
Unix-Benutzer, denen der Zugriff verweigert werden sollen (von <i>/etc/ftpusers</i>)	root bin daemon adm lp sync shutdown halt mail										
Unix-Benutzer und UIDs, denen der Zugriff verweigert werden soll	%-99 %65534-										
Unix-Gruppen und GIDs, denen der Zugriff verweigert werden soll	%-99 %65534-										
Unix-Benutzer und UIDs, denen der Zugriff <i>nicht</i> verweigert werden soll	ftp										
Unix-Gruppen und GIDs, denen der Zugriff nicht verweigert werden soll	ftp										
Speichern											

 [Zurück zu FTP-Server-Einstellungen](#)

Abbildung 8-5: Benutzer und Klassen

9 ntpd – Der Zeit Server

9.1 Funktionsweise

Der Zeitserver ist ein Dienst der sich automatisch in einem gegebenen Intervall mit einem angegebenen Referenzzeitserver im Internet verbindet, die Laufzeit der Signale berechnet, sich die aktuelle Zeit holt und durch die gemessene Laufzeit korrigiert. Dies ist die Clientseite des Servers. Die Serverseite stellt nun wiederum anderen Clients im LAN die aktuelle Zeit zur Verfügung.

9.2 Installation und automatischer Start

Wie bereits die anderen Server vorher ist auch der ntpd bei der Vollinstallation mit installiert worden. Sein Startverhalten wird über ein Start- und Stoppskript in den Runlevel Verzeichnissen unter /etc bestimmt. Unter Webmin findet man dies in den „Systemstart- und Herunterfahr Dienste“ (in System → System Start und Stopp) eingestellt. Über den Link ntp gelangt man auf die Detailansicht.

9.3 Konfiguration

Die Konfiguration umfasst nur die Angabe des Referenzservers. Dieser wird in die Datei /etc/ntp.conf eingetragen.

Ausschnitt:

```
# another protocol, the prefer keyword would cause the local host to
# disregard all other synchronization sources, unless the kernel
# modifications are in use and declare an unsynchronized condition.
#

server 130.133.1.10      # cronos.zedat.fu-berlin.de

# ...
```

10 Webmin

10.1 Was ist Webmin ?

Webmin ist ein Konfigurationstool welches modular aufgebaut ist und ständig aktualisiert und erweitert wird. Es kann nach der Installation durch einen beliebigen Webbrowser auf jedem beliebigen Rechner der mit dem Webmin Rechner vernetzt ist bedient werden.

10.2 Installation

Nach dem herunterladen des Webmin Paketes wird es einfach von der Konsole aus mit der folgenden Zeile installiert:

```
rpm -i /pfad/zum/paket/webmin-versionsnummer.rpm
```

Zum Zeitpunkt der Drucklegung war die Version 0.96 unter der Internetadresse www.webmin.com verfügbar.

Wir weisen darauf hin das Webmin noch in der Entwicklung ist. Dies ist auch an der Versionsnummer zu sehen. Wir hatten einige Male Schwierigkeiten mit einzelnen Funktionen (quotas, apache proxy) die teilweise durch neuere Versionen behoben wurden.

11 Linux Firewall

11.1 Allgemeines zur Firewall

Eine Firewall dient zur Kontrolle der Daten die einen Computer passieren wollen, dazu werden alle Datenpakete in denen die Daten verpackt sind durch die Firewall überwacht. Der Sinn dieser Überwachung ist es einen Zugriff von fremden Personen auf das eigene System abzublocken sowie der Schutz vor Fehlern der eigenen Software und unerwünschten Programmen. Durch eine Firewall wird somit der gesamte Datenfluss durch die Regeln der Firewall beschränkt. Aufgrund der zahlreichen Konfigurationsmöglichkeiten einer Firewall mit Linux eigenen Mechanismen ist es möglich das eigene System so abzudichten wie man es für nötig hält. Aber gerade durch die Vielzahl dieser Möglichkeiten ist es nicht so einfach, eine wirklich sichere Firewall zu erstellen. Die folgenden Ausführungen sollen behilflich sein um dieses Ziel dennoch zu erreichen.

11.1.1 Grundlegende Arbeitsweise einer Firewall mit Linux 2.4

Die Kommunikation also der Datenaustausch zwischen verschiedenen Rechnern bzw. Netzwerken, bedeutet das die Daten entsprechend ihrer Protokolle immer in Pakete verpackt werden. Diese Pakete werden durch die Firewall überprüft. Anhand der verschiedenen Regeln, die die Firewall beinhaltet, entscheidet diese was mit den entsprechenden Paketen geschehen soll. Die Aktionen die dann von der Firewall ausgeführt werden sind ACCEPT, DROP und REJECT. Bei ACCEPT werden die entsprechenden Pakete akzeptiert und können die Firewall passieren und weiterverarbeitet werden. Im Fall von DROP werden die Pakete verworfen und somit von der Firewall abgeblockt. Mit REJECT werden die Pakete ebenfalls verworfen teilt dem Absender jedoch durch eine Fehlermeldung die Ablehnung des Paketes mit. Eine Firewall selbst besteht aus einer Reihe von Regeln die nacheinander abgearbeitet werden. Jedes Datenpaket wird wie bei einer Checkliste mit den Regeln verglichen. Die erste Regel auf die der Vergleich zutrifft, entscheidet was mit dem Datenpaket geschehen soll. Um entscheiden zu können ob ein Paket akzeptiert wird oder nicht werden in den Firewall Regeln verschiedene Parameter abgefragt. Die wichtigsten Parameter sind das verwendete IP- Protokoll, die IP- Adressen von Absender und Empfänger des Paketes, die Portnummern sowie das Netzwerkinterface über das die Daten verschickt bzw. empfangen werden sollen.

11.1.2 Hintergrundinformationen zu IP Protokollen

Um die Funktion einer Firewall verstehen zu können ist ein Ausflug zu der Funktionsweise von IP Protokollen von Nöten.

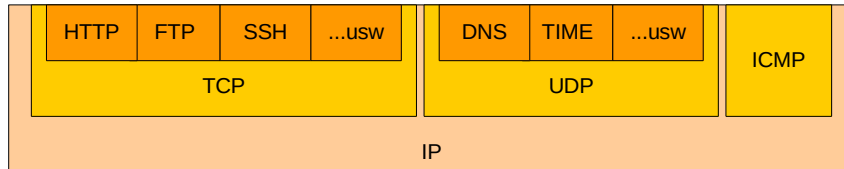


Abbildung 11-1: Verhältnis der IP Protokolle zu den Protokollen der Anwendungsebene

11.1.2.1 TCP (Transmission- Control- Protocol)

Das TCP Protokoll ist im Moment das meist genutzte Protokoll das von fast allen Internet Diensten verwendet wird. Das TCP Protokoll kennt den Begriff der Verbindung, die vor der Übertragung aufgebaut und danach wieder abgebaut werden muss. Während einer bestehenden Verbindung garantiert TCP die Integrität der Daten. Wenn während einer Verbindung einzelne Pakete verloren gehen, werden diese automatisch noch mal übertragen. Ebenfalls werden die Daten von TCP auch in die richtige Reihenfolge einsortiert bevor diese an die Anwendung weiter gegeben werden. TCP ist für eine Firewall besonders praktisch, da man den Aufbau einer Verbindung anhand von Flags im Kopf des Paketes erkennen kann. Hierdurch lassen sich Datenströme beurteilen, gehören sie zu einer Datenübertragung die durch ein Client-Programm initiiert wurde wie zum Beispiel Netscape oder versucht jemand von außen den Zugriff auf das System?

11.1.2.2 UDP (User- Datagram- Protocol)

Mit UDP werden Datenpakete von einem zum anderen Computer verschickt. Bei dieser Übertragung identifizieren sich die beteiligten Programme anhand von Portnummern. Bei UDP entfällt die Aushandlung der Verbindung, wodurch das Protokoll für Anwendungen besonders geeignet ist bei denen es auf Schnelligkeit ankommt, wie zum Beispiel bei vernetzten Dateisystemen oder Multimedia- Übertragungen. Der Nachteil bei UDP ist, das Pakete verloren gehen können und auch die Reihenfolge in der sie beim Empfänger ist undefiniert wodurch sich das Anwenderprogramm nicht auf Datenintegrität verlassen darf. Im Bezug auf die Firewall hat UDP auch Nachteile, da bei ankommenden Paketen nicht festgestellt werden kann ob es eine Reaktion auf eine Anfrage ist oder ob ein Zugriff auf das System von außen versucht wird.

11.1.2.3 ICMP (Internet- Control- Message- Protocol)

Bei ICMP werden genauso wie bei UDP nur einzelne Pakete übertragen, wobei ICMP aber nicht dem Versand von Nutzerdaten dient, sondern nur Statusinformationen über das Netzwerk oder Fehlermeldungen versendet. Im Bezug auf die korrekt arbeitende Firewall ist es wichtig das diese auf ICMP- Pakete eingeht.

11.2 Firewall mit Linux 2.4

Beim erstellen von Sicherheits- relevanten Mechanismen gibt es grundsätzlich zwei entgegensetzte Ansätze. Zum einen versucht man nicht erwünschte Ereignisse zu erkennen und auszuschalten, alles andere zu erlauben. Dieser Ansatz ist aus Sicht der zu erstellenden Firewall sehr gefährlich, da wenn ein Ereignis vergessen wird dieses automatisch erlaubt ist. Dieses ist besonders dahin gehend gefährlich weil bis jetzt unbekannte Angriffe auf das System ohne weiteres die Firewall passieren könnten. Bei der Erstellung von Firewall- Regeln geht man daher den zweiten Weg. Indem man unbekannte Ereignisse immer verbietet und unbekannte Pakete niemals annimmt. Daraus folgt das alles was erlaubt sein soll, explizit definiert werden muss. Dieses birgt aber auch einen Nachteil in sich und zwar, das solange eine Firewall unvollständig oder fehlerhaft ist, ein vernünftiger Netzwerkzugriff nicht möglich ist. Des Weiteren muss für jedes Anwendungsprogramm, welches ein neues Netzwerkprotokoll verwendet die Firewall entsprechend angepasst werden. Im Falle einer Linux Firewall werden die beiden vorgestellten Prinzipien durch so genannte Policies umgesetzt. In den nachfolgenden Erläuterungen wird ausschließlich auf den Netfilter des Kernel 2.4 eingegangen. Die Versionen der Kernel 2.0 und 2.2 „IPWADM“ und „IPCHAINS“ werden hier nicht betrachtet.

11.2.1 Firewall auf Basis „NETFILTER“ des Kernel 2.4 (IPTABLES)

Die Firewall auf Basis des Netfilter verwendet drei verschiedene Tabellen, wobei die „filter-Tabelle“ die eigentlichen Firewall- Regeln, die „nat-Tabelle“ die Regeln für Network-Adress- Translation beinhalten. Als drittes gibt es noch die „mangle-Tabelle“ in der zusätzliche Möglichkeiten der Modifikation ermöglicht werden. Wie schon erwähnt befinden sich die für die Firewall wichtigen Regeln alle in der „filter-Tabelle“, worauf nun das Augenmerk gelegt werden soll. Jede dieser Tabellen besteht aus so genannten Chains (Ketten). Diese Chains werden „INPUT“, „OUTPUT“ und „FORWARD“ genannt. Alle Daten die für den Linuxrechner bestimmt sind durchlaufen die INPUT- Chain, alle Daten die der Linuxrechner erzeugt die OUTPUT- Chain. Die FORWARD- Chain ist für Daten die direkt vom LAN ins Internet und umgekehrt geschickt werden.

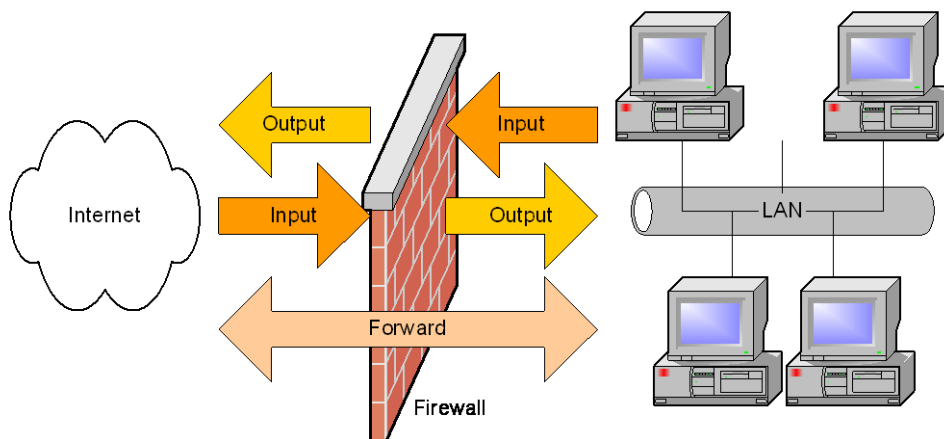


Abbildung 11-2: Darstellung der Ketten

11.2.2 Aufruf-Konventionen von iptables

Grundsätzlich gilt:

- Kommandos bestehen aus einem Grossbuchstaben, z.B. -L oder der entsprechenden Langform z.B. --list
- Targets (d.h. Ziele oder Aktionen) bestehen aus einem großgeschriebenen Wort, z.B. DROP
- Chains bestehen aus einem großgeschriebenen Wort, z.B. INPUT
- Tabellen sind Worte in Kleinbuchstaben, z.B. filter
- Optionen bestehen aus Kleinbuchstaben, z.B. -t oder --source-port

11.2.3 Typische Kommandos (Auswahl)

! Ein vorangestelltes "!" bedeutet Negation, d.h. der nachfolgende Parameter darf nicht mit den Daten eines Paketes übereinstimmen. Ohne "!" wird stets auf Übereinstimmung getestet.

[...] Alle in eckigen Klammern stehenden Werte sind optional

<...> Das in spitzen Klammern stehende Wort steht stellvertretend für den stattdessen einzusetzenden Inhalt

Tabelle 11-1: iptables Befehle

Kommando	Bedeutung
-A <chain> <regel>	Anfügen einer neuen Regel am Ende einer Chain/Tabelle
-D <chain> <regel>	Löschen einer Regel aus einer Chain/Tabelle
-C <chain> <regel>	Testen eines Paketes mit bestimmten Bedingungen auf eine Chain/Tabelle
-R <chain> <nr> <regel>	Ersetzen einer Regel durch eine neue
-I <chain> <nr> <regel>	Einfügen einer Regel in eine Tabelle/Chain
-L [<chain>]	Auflisten aller Regeln einer Tabelle/Chain evtl. mit -Z
-F [<chain>]	Alle Regeln einer Chain löschen
-Z [<chain>]	Löschen der Zähler einer Chain
-N <chain>	Neue benutzerdefinierte Chain anlegen
-X <chain>	Benutzerdefinierte Chain löschen
-P <chain> <ziel>	Standardverhalten einer Chain festlegen
-E <chain> <chain-neu>	Umbenennen einer Chain

Tabelle 11-2: Generelle, begleitende Optionen

Kommando	Bedeutung
-t <tabelle>	Auswahl einer Tabelle (filter, nat, mangle); "filter" ist die Standard-Tabelle, falls diese Option nicht gewählt wurde. Hierbei wird das diese Tabelle "managende" Modul [iptables_<tabelle>] geladen, sofern der Kernel mit automatischem Modul-Loading konfiguriert ist.
-v	Mehr ausgeben...
-n	Numerische Ausgaben bei Auflistungen
-x	Exakte Zahlenangaben anstelle von Kilo, Mega, Giga...
-h	Hilfe-Meldungen und Optionen ausgeben (in Verbindung mit -m oder -j werden die mit dem jeweiligen Modul zur Verfügung stehenden zusätzlichen Optionen angezeigt).
-m <modul>	Zusätzliche Optionen bereitstellen, die im angegebenen Modul verankert sind. Hierbei wird der Modulname ohne vorangestelltes "ipt_" und ohne Erweiterung angegeben (z.B. "mac" zum Laden des Moduls "ipt_mac.o"). Besonders hilfreich ist in diesem Zusammenhang die Hilfe-Funktion (-h), die in Verbindung mit einem Modul dessen Parameter und Optionen auflistet.

11.3 Grundlegende Konfiguration der Firewall

Die folgenden Ausführungen beziehen sich nicht auf das Projekt, eine Firewall für einen Server zu erstellen sondern soll nur die grundlegenden Prinzipien aufzeigen. Die Regeln für eben dieses Projekt werden später mit dem GUI- Tool „Firewall Builder“ erstellt und erläutert.

Vor dem erstellen von neuen Firewall- Regeln sollte man, um Schwierigkeiten zu vermeiden, eventuell vorhandene Regeln die bereits vom System erstellt wurden ausschalten. Dieses erreicht man in dem man in der Datei die später die Regeln enthalten soll als erstes den folgenden Eintrag macht.

```
iptables -F
```

Den vorgestellten Prinzipien folgend werden anschließend alles gesperrt, um später durch entsprechende Regeln einzelne Datenpakete die, die Firewall passieren dürfen wieder freizugeben. Um dieses zu erreichen verwendet man folgende Regeln.

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

Nachdem man nun alles gesperrt hat, macht man sich daran die einzelnen Prozesse die gewünscht sind wieder freizugeben. Als Beispiel hierfür soll die Verbindung zum WWW betrachtet werden. Bevor man sich daran begibt muss man aber wissen welche entsprechenden Portnummern zu den jeweiligen Prozessen gehören. Hierzu dient die folgende Liste die eine Auswahl der Portnummern ist. Die vollständige der von Linux unterstützten Ports findet man in der Datei `/etc/services`.

21	FTP	(Datenübertragung)
22	SSH	(SecureShell)
23	TELNET	(unsichere Alternative zu SSH)
25	SMTP	(Mail- Versand)
43	WHOIS	(Verzeichnis der Inhaber und Betreiber von Internet- Domains)
53	DNS	(Zuordnung von Domain- Namen und IP- Adressen)
79	FINGER	(Abfrage von Benutzerinformationen)
80	HTTP	(Verbindung zum WWW)
110	POP3	(Mail- Empfang)
119	NNTP	(Usenet- News- Versand und Empfang)
143	IMAP	(Mail- Empfang)
443	HTTPS	(sichere Verbindung zum WWW)

Wie aus der Liste zu ersehen ist wird bei einem Client der zum Beispiel mit Netscape eine Verbindung zu einem Webserver herstellen will der Port 80 verwendet. Um nun eine Regel zu erstellen benutzt man nun folgenden Befehl.

```
iptables -A OUTPUT -p tcp --sport 1024: --dport 80 -j ACCEPT
```

Die Option `-A OUTPUT` hängt die neue Regel an die Output Chain an, das `--sport 1024:` steht für den Source Port. Dieser muss mindestens 1024 sein, mit dem angehängten Doppelpunkt erreicht man das auch alle darüber liegenden Ports erlaubt sind. Durch diese Regel hat man nun erreicht das der Client ein Paket an den Webserver schicken kann.

Da jetzt zwar dieser Weg frei ist, kann man aber in diesem Moment noch nichts empfangen. Hierfür ist nun eine weitere Regel erforderlich.

```
iptables -A INPUT -p tcp --sport 80 --dport 1024: ! --syn -j ACCEPT
```

Wie zu erkennen ist sind hier nun die Absender- und Empfänger –ports vertauscht. Die Option `! --syn` überprüft bestimmte Flags im Kopf des TCP- Paketes und erkennt daran das erste Paket einer neuen Verbindung. Im Klartext bedeutet dies das alle Pakete die zu einer bestehenden Verbindung gehören erlaubt sind, ein Aufbau einer neuen Verbindung von außen aber verweigert wird, also Programme auf dem eigenen System Verbindungen aufbauen darf, fremde Rechner von außerhalb aber nicht. Da es sich hierbei aber um einen relativ einfachen Mechanismus handelt, verwendet man lieber ein separates Modul zur Verbindungsüberwachung. Dieses erreicht man durch hinzufügen folgender Regeln.

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Durch diese beiden Regeln merkt sich die Firewall alle bestehenden Verbindungen. Gelangt jetzt ein Paket an die Firewall überprüft diese ob es zu einer bestehenden bzw. bekannten Verbindung gehört. Wird erkannt das die Verbindung bekannt ist, so wird

das Paket ohne weiteres nachfragen zugelassen. Ebenfalls werden hierdurch Pakete erkannt die als verwandt gelten. Um so genannte verwandte handelt es sich zum Beispiel um ICMP- Fehlermeldungen oder die Datenkanäle einer FTP- Verbindung. Bei dieser Art der Überwachung kann man die Überprüfung mit der Option `!-syn` unterlassen.

Anhand der vorgestellten Regeln für den Port 80 ist es nun möglich weitere Regeln für die anderen Ports zu erstellen, die die Firewall passieren dürfen. Eine Ausnahme bildet aber der Datenverkehr über FTP, weil dort eine Verbindung zu den oberen Ports aufgebaut wird. Man unterscheidet zwischen dem aktiven und passiven Modus. Beim aktiven Modus handelt es sich um eine Verbindung vom FTP- Server zu uns und im passiven Modus baut ein FTP- Client über die oberen Ports eine Verbindung auf. Normalerweise ist dieses recht unsicher und beinhaltet Sicherheitsrisiken. Durch die erstellten Regeln zur Überwachung der Verbindungen verhindert man diese Risiken aber.

11.3.1 Verbindungen zwischen Programmen auf einem Rechner

Um die IP- basierte Kommunikation zwischen Programmen auf dem eigenen Rechner zu ermöglichen, wird ein besonderes Netzwerkinterface benutzt. Hierbei handelt es sich um das so genannte „Loopback Device“ das auch kurz mit „lo“ bezeichnet wird. Um nun Programmen die Möglichkeit zu geben, miteinander kommunizieren zu können, sind weitere Regeln nötig.

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

Durch die Optionen `-i` bzw. `-o` werden die Pakete die über das angegebene Netzwerkinterface empfangen (input) oder gesendet (output) werden eingeschränkt.

11.3.2 Betrieb von Servern hinter der Firewall

Da es sich bei einem Betriebssystem wie Linux anbietet eigene Server einzurichten und auf diese über das Internet zugreifen zu können, müssen auch hierfür entsprechende Firewall- Regeln erstellt werden. Als Beispiel soll hierfür HTTP und SSH dienen. Die entsprechenden Regeln sehen dann folgendermaßen aus.

```
iptables -A INPUT -p tcp -s xxx.xxx.xxx.xxx/24 --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
```

Aus diesen Regeln ist ersichtlich das man für jeden Server den man aufsetzt zwei Regeln erforderlich sind. Also jeweils eine für ausgehende und eine für eingehende Pakete. Mit der Option `-s` und einer IP Adresse, die hier durch `xxx.xxx.xxx.xxx` dargestellt ist, kann man die Quelle (source) einschränken. Im konkreten Beispiel würden alle IP- Adressen des Bereiches `xxx.xxx.xxx.0` bis `xxx.xxx.xxx.255` über SSH eine Verbindung zum System aufbauen können. Durch die Option `-d xxx.xxx.xxx.xxx` könnte man der Verbindung noch ein Ziel (destination) angeben. Für alle weiteren Server die auf dem Rechner laufen sollen, geht man nach dem selben Prinzip vor.

11.3.3 Regeln für DNS (Domain Name Service)

Der DNS bedarf einer besonderen Beachtung, da dieser immer notwendig ist, das beruht darauf das die Namensauflösung eine wesentliche Voraussetzung für die Internet-Kommunikation ist. Wird eine Anfrage an einen DNS Server gestellt, so wird diese immer über zuerst über UDP ausgeführt. Wenn die Antwort für diese Anfrage aufgrund ihrer Größe mit UDP nicht ausgeführt werden kann, wird die Anfrage nochmals über TCP wiederholt, da hierüber größere Datenmengen übertragen werden können. Für diese Besonderheiten gelten folgende Regeln.

```
iptables -A OUTPUT -p udp --sport 1024: --dport 53 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 1024: --dport 53 -j ACCEPT
```

Aufgrund der schon erwähnten Besonderheiten von UDP in Bezug auf eine Firewall, das genau diese Firewall nicht feststellen kann ob ein UDP Paket zu einer bestehenden Verbindung gehört. Aus diesem Grund bedeutet es für die Erstellung der Firewall besondere Aufmerksamkeit. Wenn nun ein DNS Server Kontakt mit dem eigenen Rechner aufnimmt geschieht das von Port 53 aus. Das Ziel ist einer der oberen Ports auf dem eigenem System, dies geschieht aber nur wenn man keinen eigenen DNS Server betreibt. Wenn man nur auf einen einzigen DNS Server zugreift, wie z.B. den des Internetproviders, erlaubt man nur UDP Pakete von genau dieser IP Adresse. Die Regeln sehen dann wie folgt aus.

```
nameserver=xxx.xxx.xxx.xxx
iptables -A INPUT -p udp -s $nameserver --sport 53 -j ACCEPT
iptables -A INPUT -p tcp -s $nameserver --sport 53 -j ACCEPT
```

Wird im eigenem System ein DNS Server betrieben wird, kann man den lokal verwendeten Port konfigurieren. In diesem Fall werden UDP Pakete aus dem ganzen Internet akzeptiert, jedoch nur an diesem einen UDP Port.

```
iptables -A INPUT -p udp --sport 53 --dport 7531 -j ACCEPT
```

Wenn kein eigener DNS Server wird und bei veränderlichem fremden Server wie z.B. bei einer Modem Einwahlverbindung ist es möglich, ein Script zu erstellen um nach jeder neuen Interneteinwahl die Firewall zu aktualisieren. Auf diese Möglichkeit wird hier aber nicht näher eingegangen, da es nicht Bestandteil unseres Projektes ist.

11.3.4 Firewall und ICMP

Datenpakete die ICMP verwenden müssen in Bezug auf die Firewall noch besonders beachtet werden, da diese wie schon erwähnt, Informationen über den Netzwerkstatus liefern und Fehlermeldungen übertragen. Bei ICMP wird anders wie bei TCP und UDP nicht mit Ports gearbeitet, sondern mit Nachrichtentypen und einem eventuellen Subtyp. An diesen Gegebenheiten kann die Firewall erkennen worum es hierbei geht und kann somit selektiv filtern. Ein Beispiel hierfür ist z.B. `echo-request` und `echo-reply` welche Frage und Antwort von PING sind. PING benutzt man um zu überprüfen ob ein Rechner korrekt an ein Netzwerk angeschlossen ist oder nicht. Mit den folgenden Regeln erlaubt man der Firewall genau diese passieren zu lassen.

```
iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

Will man den umgekehrten Weg auch freigeben, gibt man noch folgende Regeln ein.

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

Ein weiterer Nachrichtentyp ist `destination-unreachable` mit seinen zahlreichen Subtypen, dieser teilt einem Rechner mit das eine bestimmte Resource nicht erreichbar ist. Dieser Nachrichtentyp sollte auf jeden Fall die Firewall passieren dürfen. Insbesondere der Subtyp `fragmentation-needed` ist für die Kommunikation von besonderer Bedeutung, denn unter besonderen Umständen kann eine fehlende Erlaubnis in diesem Fall zu undurchsichtigen Fehlermeldungen kommen. Um diesem Fall aus dem Wege zu gehen sollten nachfolgende Regeln in die Firewall implementiert werden.

```
iptables -A OUTPUT -p icmp --icmp-type destination-unreachable -j
ACCEPT

iptables -A INPUT -p icmp --icmp-type destination-unreachable -j
ACCEPT
```

11.3.5 Abschließende Regeln einer Firewall

Zum Abschluss muss man noch einige abschließende Regeln erstellen um die bisher noch nicht erkannten Datenpakete zu verbieten. Des weiteren sind noch Regeln zur Protokollierung des Datenverkehrs notwendig. Die folgenden Regeln sollen nur Beispiele sein um einen Datenverkehr zu protokollieren bzw. zu verbieten. Die Verbotende Regel muss auf jeden Fall am Ende der Regeln stehen.

```
iptables -A INPUT -j LOG
iptables -A OUTPUT -j LOG
iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
```

Abschließend muss noch erwähnt werden das für NAT (Network Address Translation) wenn es denn gewünscht oder gefordert wird einige Regeln erstellt werden müssen. In unserem besonderen Fall war dies aber nicht Bestandteil des Projektes. Für genauere Informationen lesen Sie die entsprechenden Dokumentationen der Betriebssysteme.

11.3.6 Speichern und automatisches ausführen der Regeln

Da wir wie schon erwähnt, die Firewall Regeln bei unserem Projekt mit dem GUI Tool „Firewall-Builder“ erstellen gehen wir in diesem Abschnitt der Dokumentation nicht näher auf diesen Punkt ein. Die entsprechenden Anleitungen entnehmen Sie bitte den Handbuchseiten bzw. der einschlägigen Lektüre oder HOWTO's.

11.4 Erstellen einer Firewall mit dem GUI- Tool „Firewall-Builder“

Um mit dem Firewall Builder arbeiten zu können laden, haben wir uns zu Anfang erst einmal das entsprechende RPM Paket von der Internetseite www.fwbuilder.org herunter geladen. Auf dieser Seite findet man auch entsprechende Dokumentationen zu dieser Software. Nachdem wir dieses getan hatten, installierten wir das RPM Paket mit dem Paket-Manager von RedHat 7.2. In den nun folgenden Ausführungen gehen wir aus Sicherheitsgründen nicht auf die detaillierte Einrichtung der Firewall unseres Projektes ein.

Die genaue Beschreibung befindet sich im Benutzerhandbuch, das nicht für die Öffentlichkeit zugänglich ist.

11.4.1 Basiskonfiguration

Bevor wir den Firewall Builder das erste Mal starteten, legten wir in `/etc` als künftiges Arbeitsverzeichnis für die Applikation das Directory `/etc/fwbuilder` an. Dort sollten später die Konfigurationsdatei des Tools sowie die erstellten Firewall-Regeln lagern.

Jetzt starteten wir den Firewall Builder. Als erstes galt es, einige grundlegende Einstellungen für die Applikation selbst zu treffen. Dazu riefen wir den Menüpunkt Edit/Options auf. Unter General/Paths des daraufhin erscheinenden Popup-Fensters trugen wir den Pfad zu unserem

Arbeitsverzeichnis - also `/etc/fwbuilder` - ein. Die Einstellungen unter Network haben wir bei den Defaultwerten belassen: Also je 10 Sekunden Timeout und einen Wiederholungsversuch.

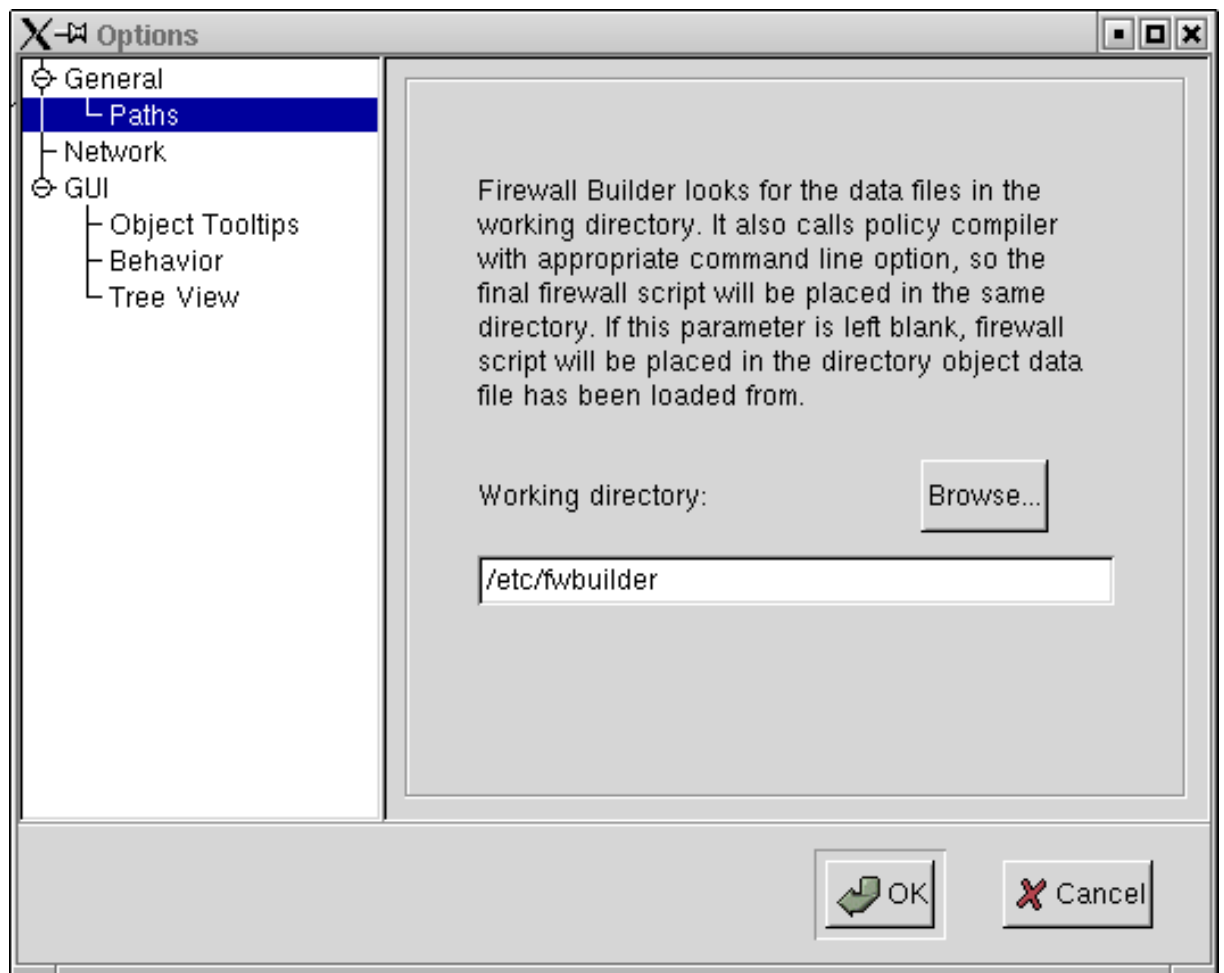


Abbildung 11-3: Angabe des Arbeitsverzeichnisses

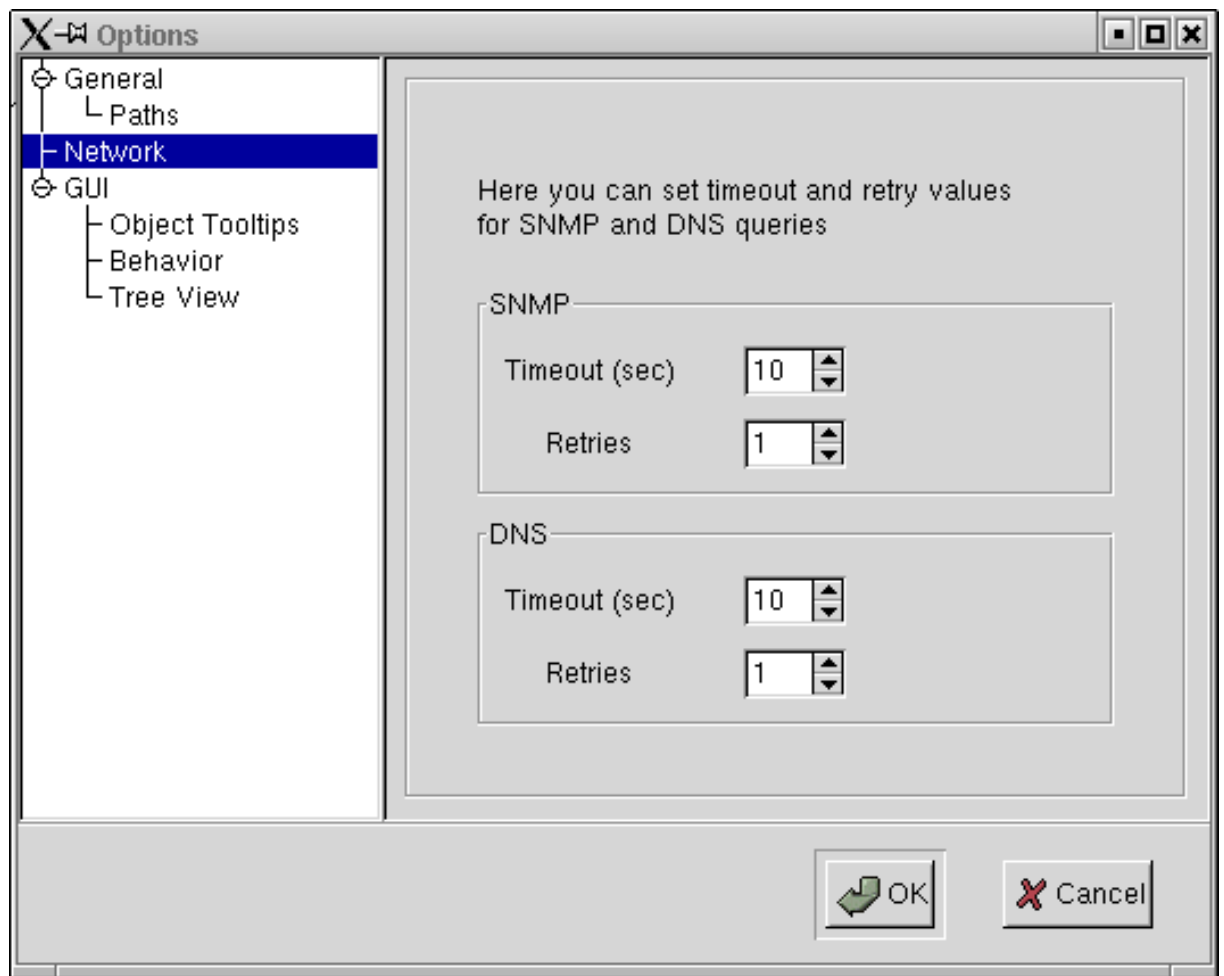


Abbildung 11-4: Default- Einstellungen unter Network

Unter GUI/Behavior stellten wir die automatische Sicherung aller Einstellungen beim Wechsel zwischen den Objekten ein. Die Optionen für <Object Tooltips> und <Tree View> haben wir außer Betracht gelassen, da diese für die grundsätzliche Funktion nicht ausschlaggebend sind. Allerdings erwiesen sich die eingestellten Vorgaben bei der weiteren Arbeit erfahrungsgemäß als hilfreich.

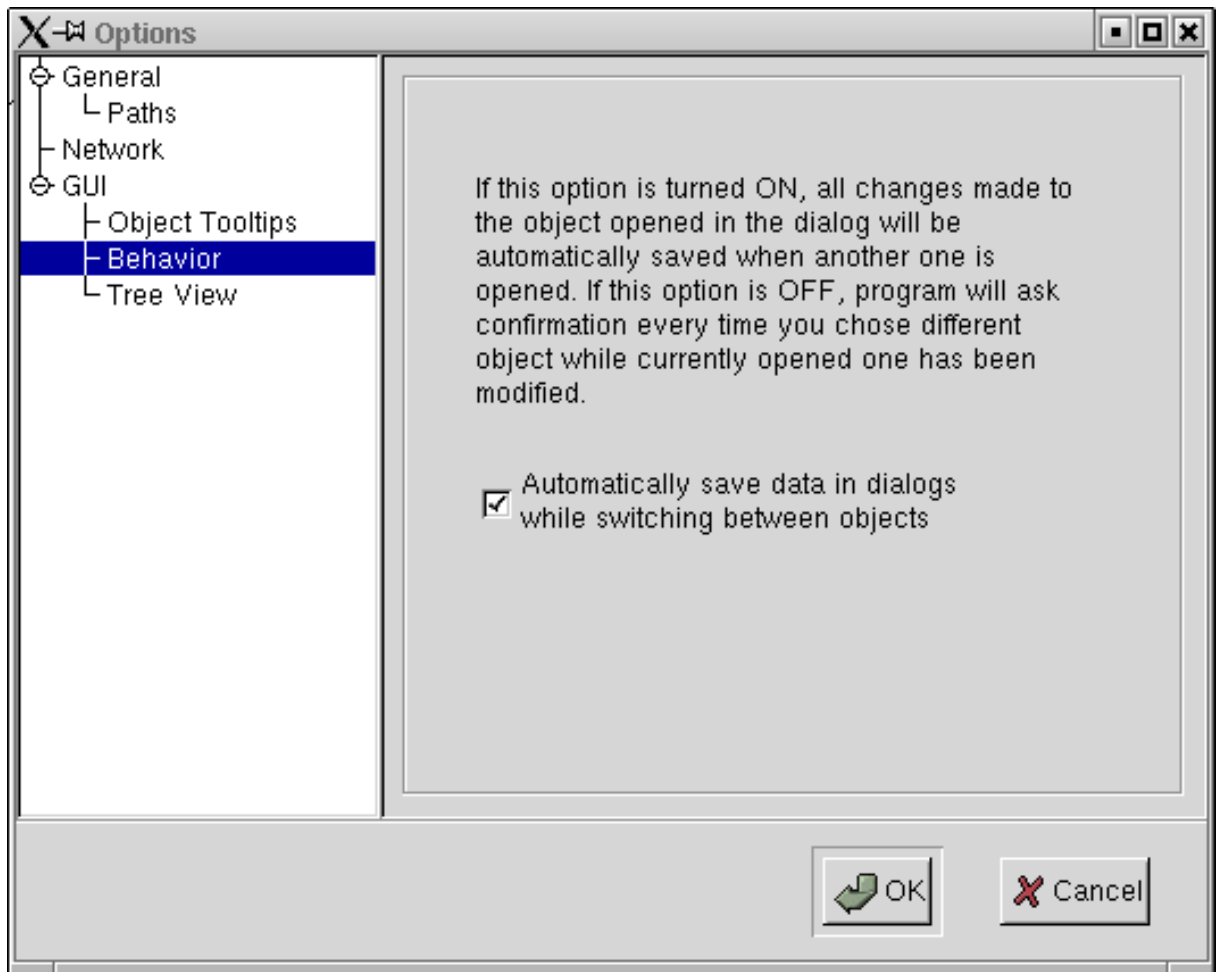


Abbildung 11-5: Automatisches Speichern beim Wechsel zwischen einzelnen Objekten

11.4.2 Erstellen des Firewall Objektes

Ein wesentliches Stichwort beim Umgang mit dem Firewall Builder sind Objekte. Bei der weiteren Konfiguration baut das Tool auf die Definition diverser Objekte auf. Dazu zählen Netzwerke und Hosts ("Objects"), Protokolle und Ports ("Services"), sowie Zeitspannen ("Time").

Das wichtigste davon stellt das Firewall-Objekt selbst dar. Dies ist also der Rechner, den es über eine zugeordnete Policy zu schützen gilt. Daher erstellten wir als erstes über den Menüpunkt Insert/Firewall ein entsprechendes Objekt.

Dieses muss über insgesamt fünf Reiter mit Einstellungen versorgt werden. Auf dem Reiter <General> trugen wir eine Bezeichnung für das Objekt, hier „Firewall“ sowie die entsprechende Netzwerkadresse ein. Als unterstützte Firewall-Software wählten wir Iptables, die anderen Werte blieben auf den Voreinstellungen.

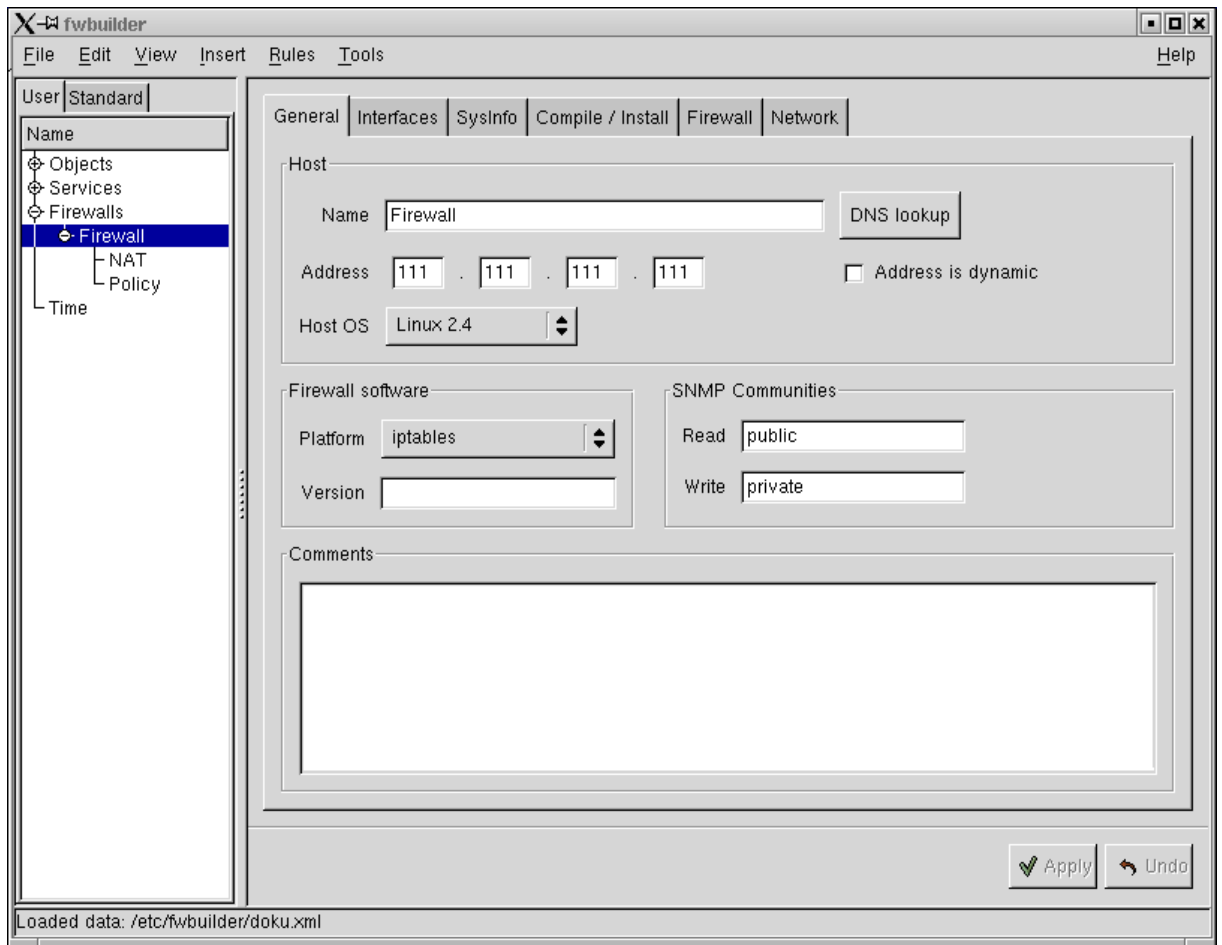


Abbildung 11-6: Erstelltes Firewallobjekt

Als nächster Punkt wurden unter dem Reiter <Interfaces> die Netzwerkschnittstellen (Netzwerkkarten) eingetragen. Dieses wurde erreicht indem wir den <New> Button betätigten. Woraufhin das folgende Fenster erschien.

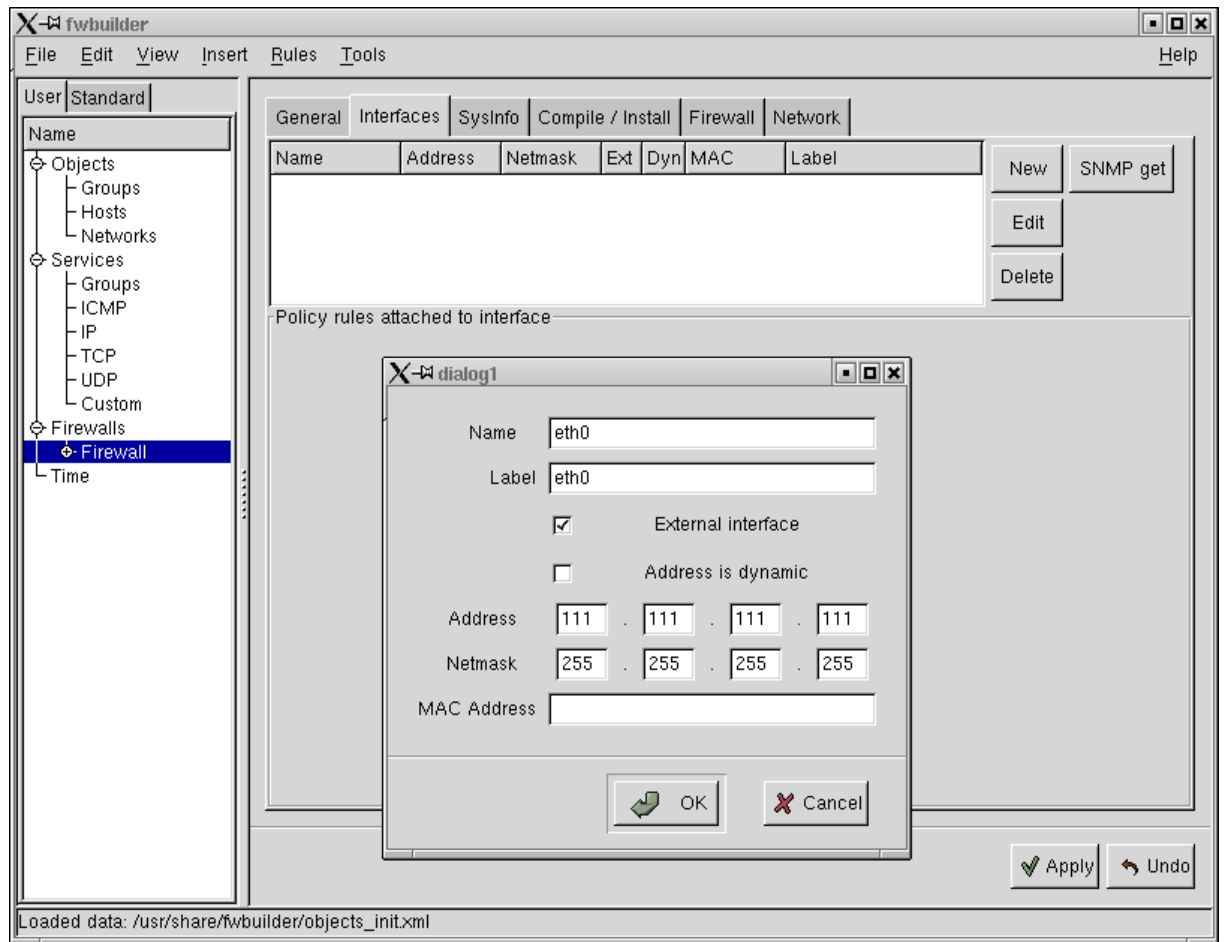


Abbildung 11-7: Einrichtung der Netzwerkkarten

In der nun aufgehenden Dialogbox trugen wir den Namen der Netzwerkkarte, einen Label (nicht unbedingt erforderlich) sowie die IP Adresse und die Netzmaske ein. Außerdem machten wir einen Haken in das Feld <External Interface> und schlossen die Dialogbox über <OK>. Diese Einstellungen wiederholten für die weiteren Schnittstellen <eth1> und das Loopback Device <lo>. Beim Loopback Device wurde allerdings der Haken im Feld <External Interface> weggelassen.

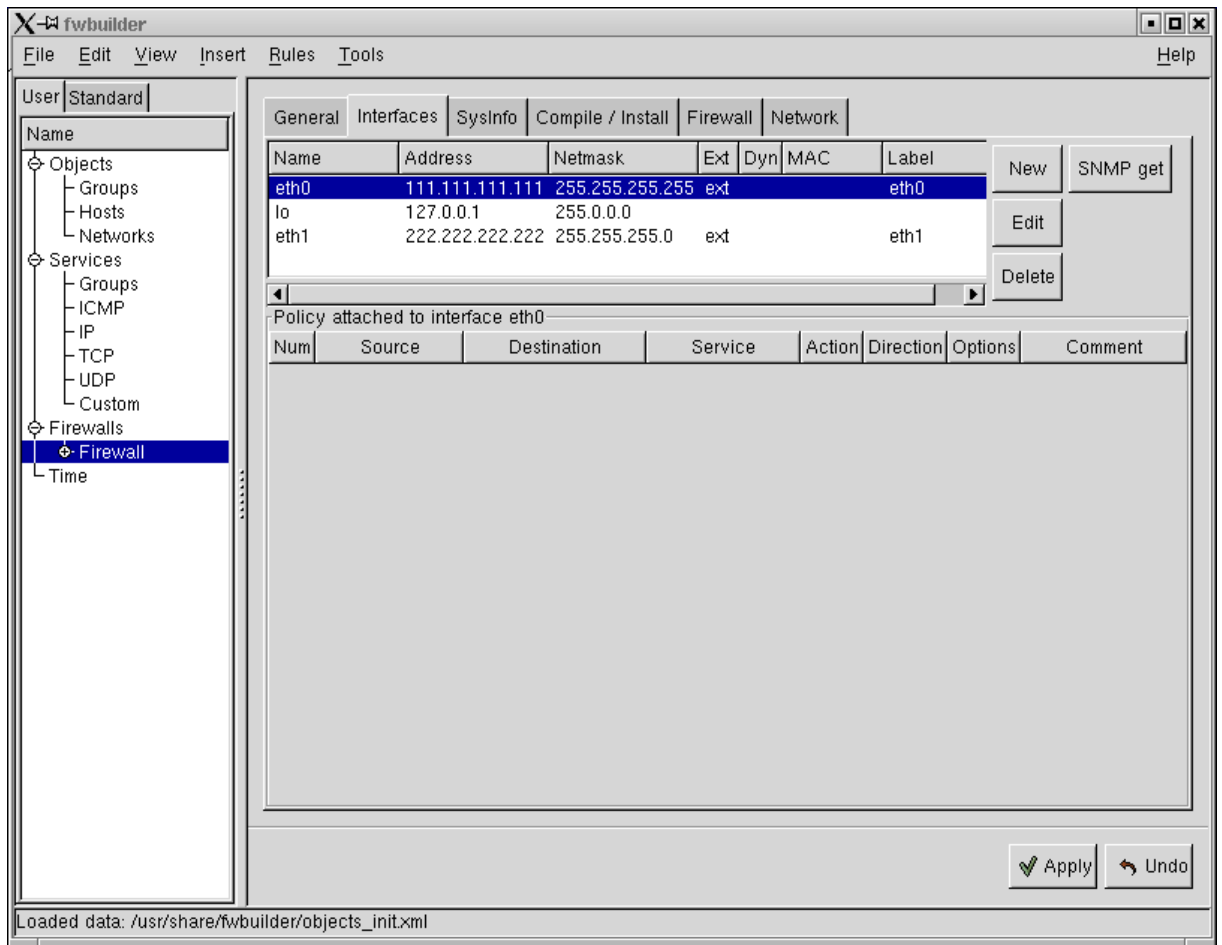


Abbildung 11-8: Fertig eingefügte Netzwerkschnittstellen

11.4.3 Kompilierung und Installation

Der Regelcompiler liegt nach einer Standardinstallation von Firewall Builder im Verzeichnis `/usr/bin`. Da wir Regeln für die Iptables Firewall erstellten, gaben wir als Pfad zum Compiler also `/usr/bin/fw-iptables` an.

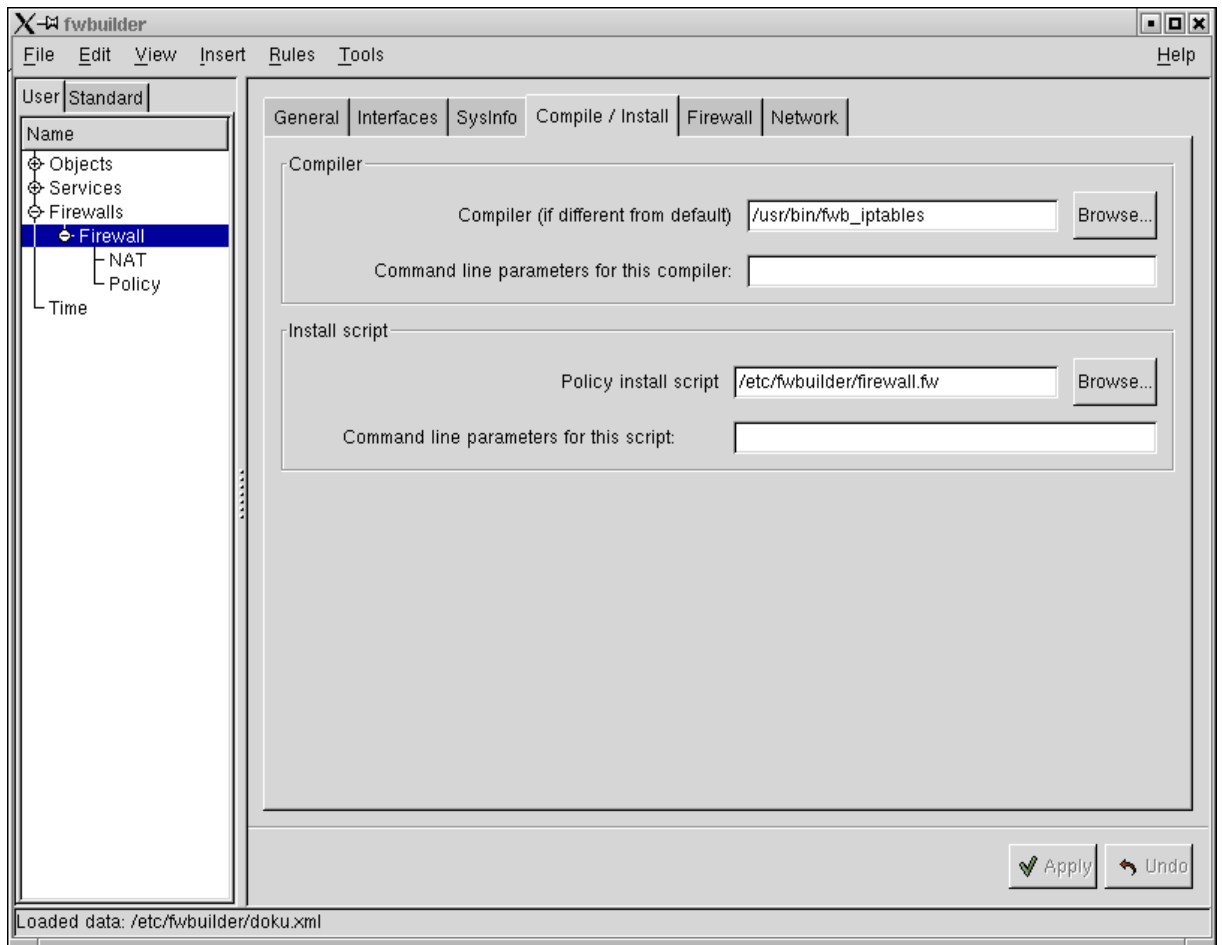


Abbildung 11-9: Eingabe der Pfade für den Compiler und das Installationsskript

Als Installationsskript haben wir, direkt das von Firewall Builder später erstellte Konfigurationsskript angegeben. Es liegt im Arbeitsverzeichnis der Applikation - bei uns also `/etc/fwbuilder` - und trägt den Namen des Firewall Objekts mit der Endung `.fw`.

Nachdem wir diese Grundeinstellungen erledigt hatten, speicherten wir den momentanen Status über den Menüpunkt `<File/Save As>` als `/etc/fwbuilder_rules.xml`.

In der folgenden Phase haben wir die Netzwerke eingerichtet an die der Server angeschlossen werden soll. Dieses erreicht man im Menü `<Insert>` unter `<Network>`. Im darauf folgenden Fenster haben wir dann den Namen des Netzwerkes, die IP-Adresse und die Netzmaske angegeben.

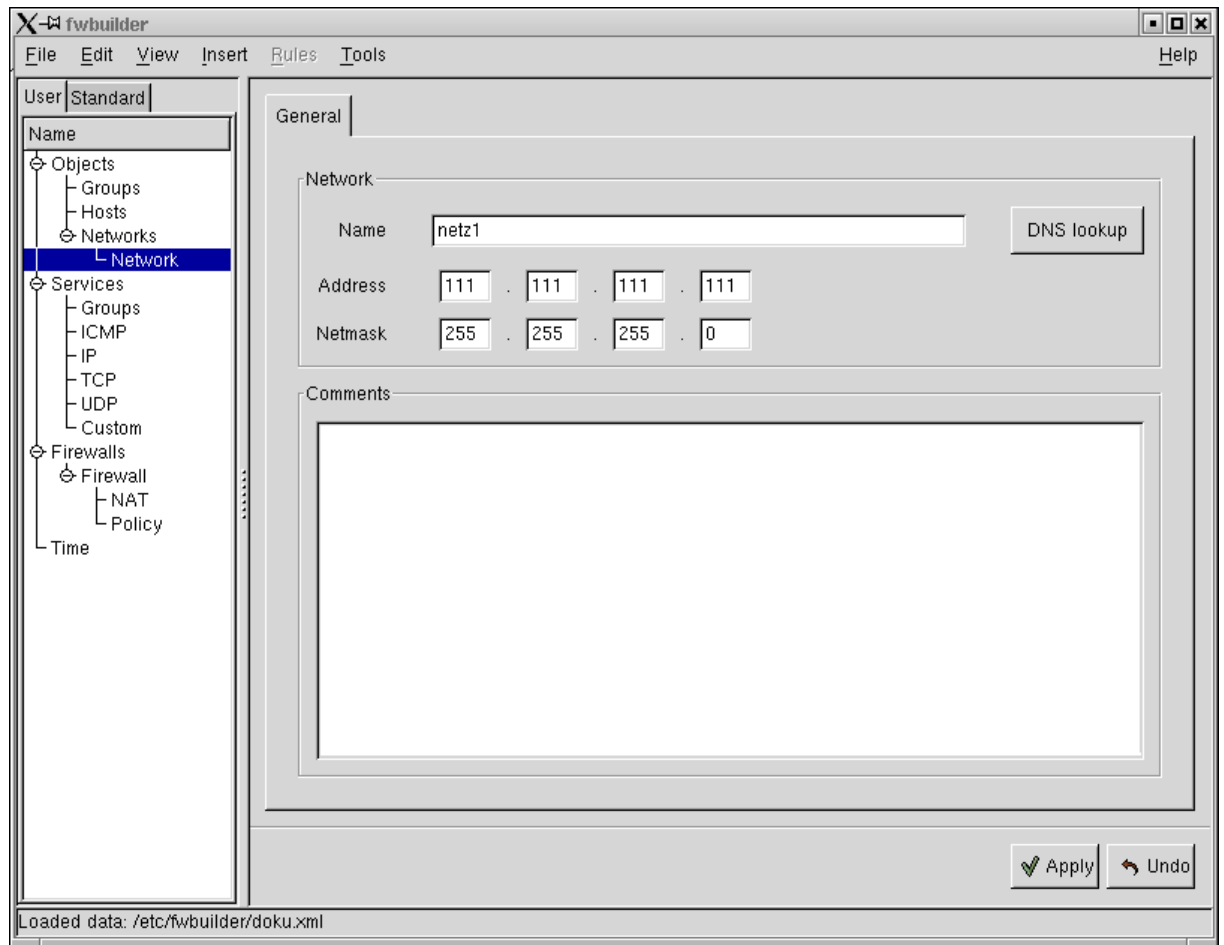


Abbildung 11-10: Einrichtung des 1. Netzwerkes

Dieses wiederholen wir ebenfalls für das zweite Netzwerk.

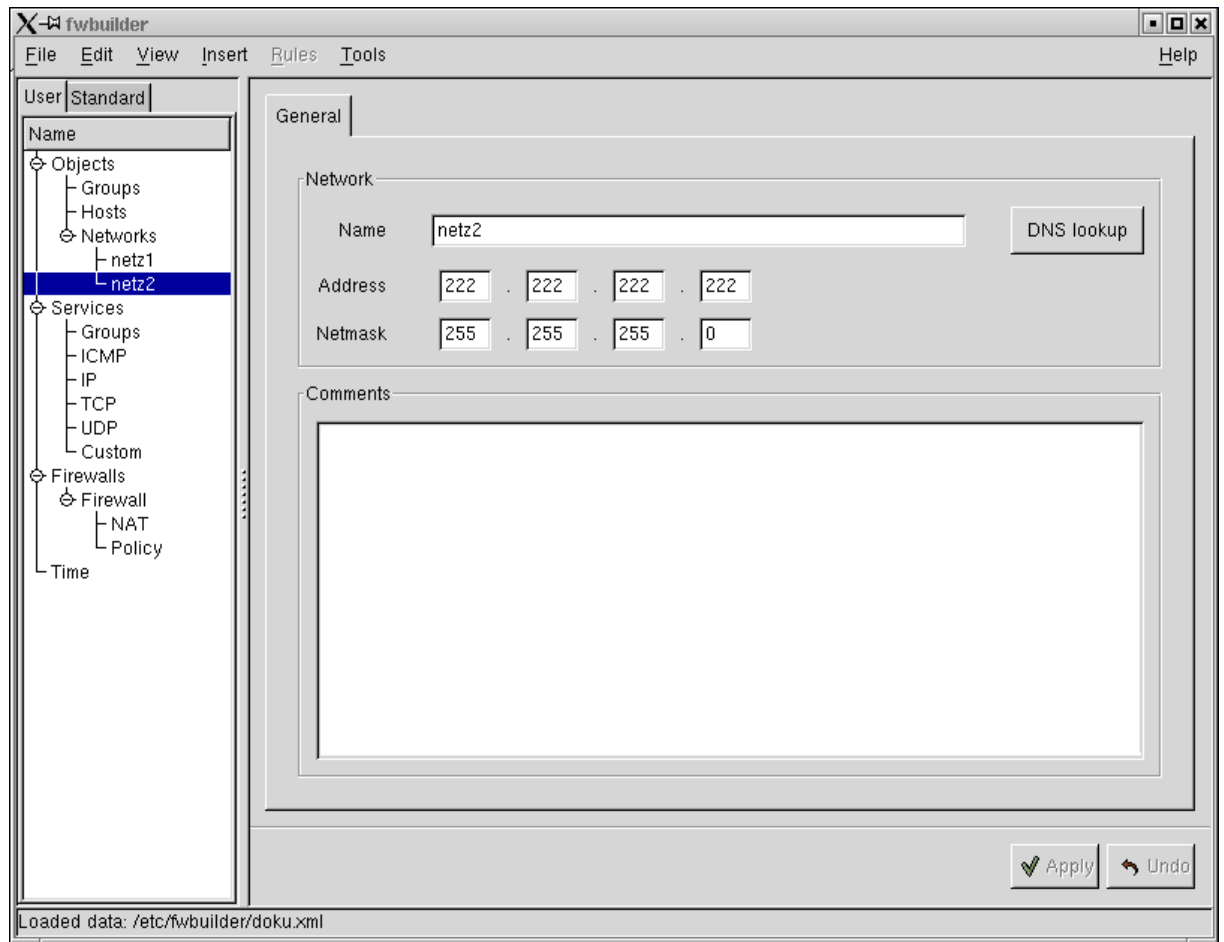


Abbildung 11-11: Fertig eingerichtete Netzwerke

11.4.4 Erstellen der Regeln für die Netzwerkschnittstellen

Um nun die Regeln zu erstellen klickt man mit der rechten Maustaste auf das graue Feld. Worauf das folgende Fenster erscheint. Nachdem dieses geschehen ist, zieht man per Drag and Drop (linke Maustaste gedrückt halten) die entsprechenden Objekte in die Felder unterhalb von – Source, Destination, Service – hiernach werden dann noch mit der rechten Maustaste auf die Felder – Action, Direction, Options, Comment – geklickt, wo die entsprechend Gewünschten Optionen ausgewählt werden.

Folgende Möglichkeiten ergeben sich:

Source: Alle unter Objects und Firewalls eingerichteten Objekte und Firewalls
 Destination: Alle unter Objects und Firewalls eingerichteten Objekte und Firewalls
 Service: Alle unter Standard oder User eingerichteten Services
 Action: Auswahlmöglichkeiten - Deny, Accept, Reject
 Direction: Auswahlmöglichkeiten - Inbound, Outbound, Both(Input, Output, Both)
 Options: Auswahlmöglichkeiten – logging on/off
 Comment: Textfeld zum eintragen eines Kommentars

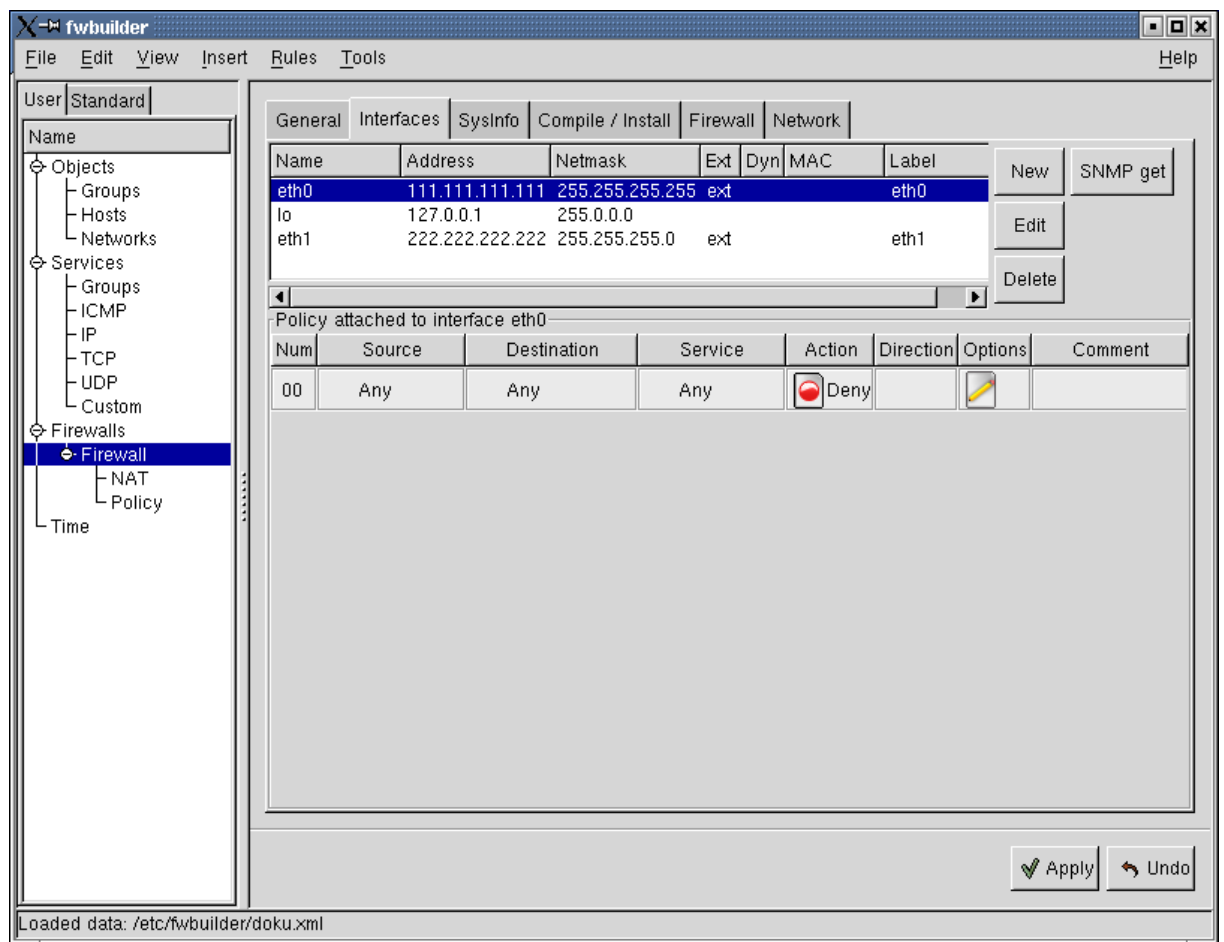


Abbildung 11-12: Einrichtung der Regeln für die Netzwerkschnittstellen

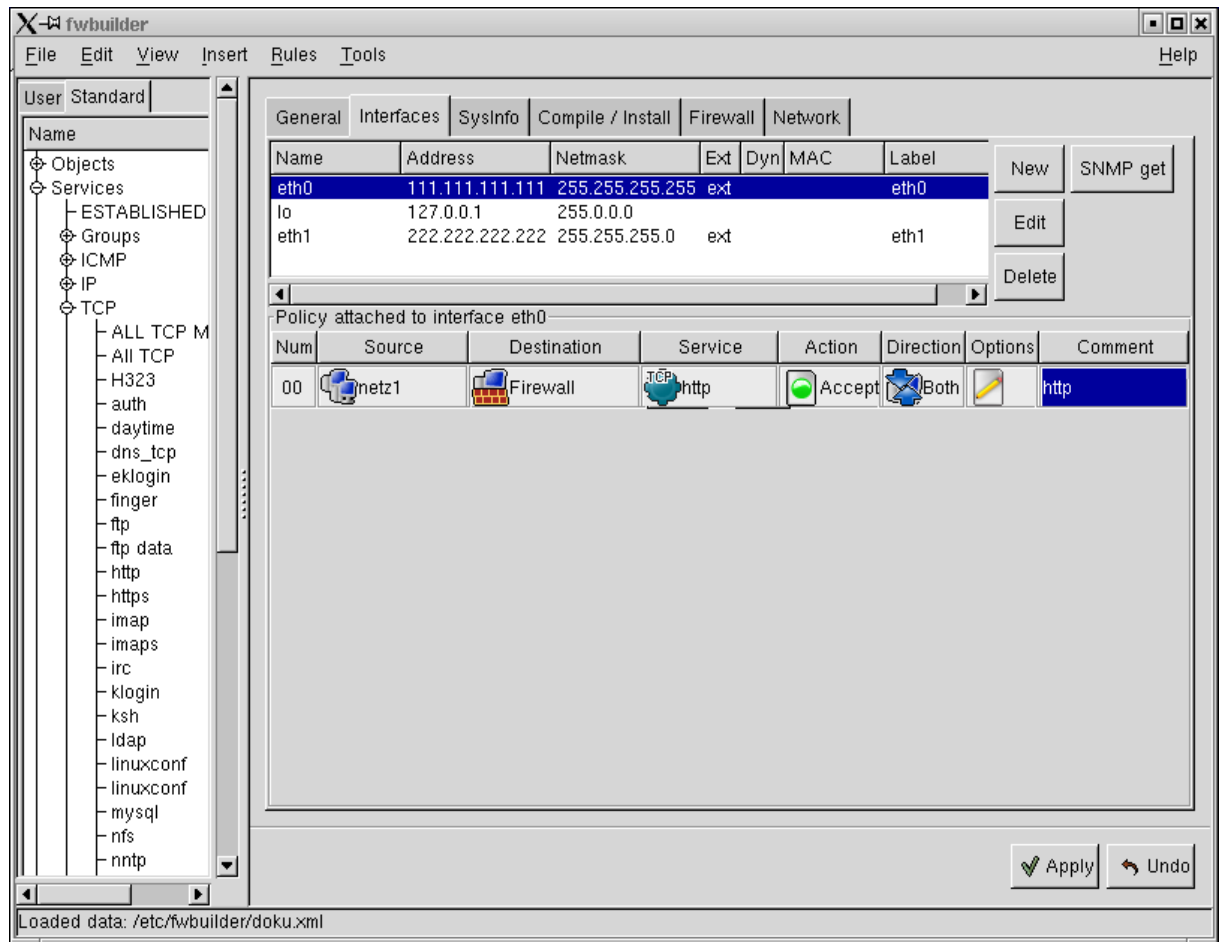


Abbildung 11-13: Eine fertig eingerichtete Regel für eth0

Für das Loopback Device wird alles freigegeben, da es sich um die so genannte und schon erwähnte Pseudoschnittstelle für lokale Anwendungen handelt.

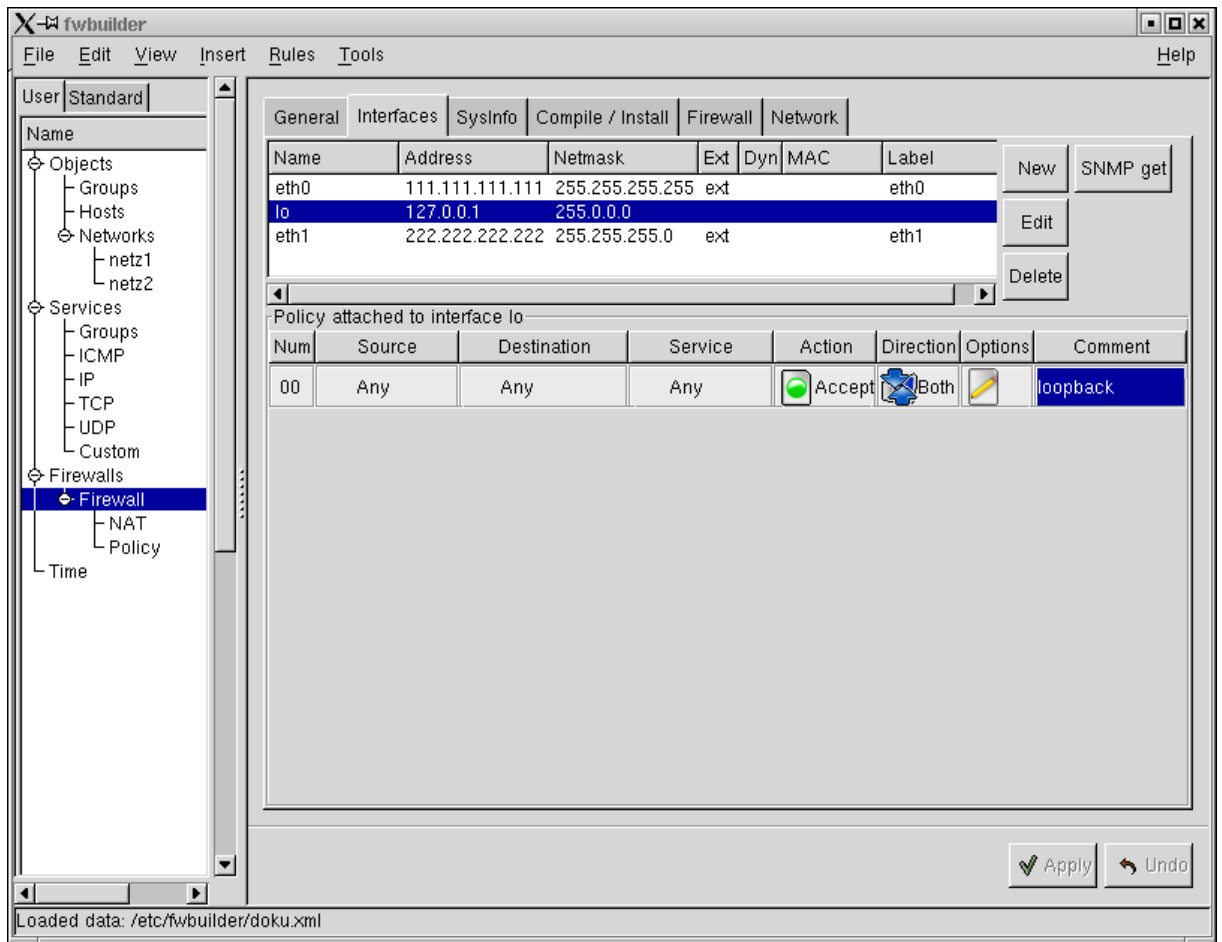


Abbildung 11-14: Regel für das Loopback Device

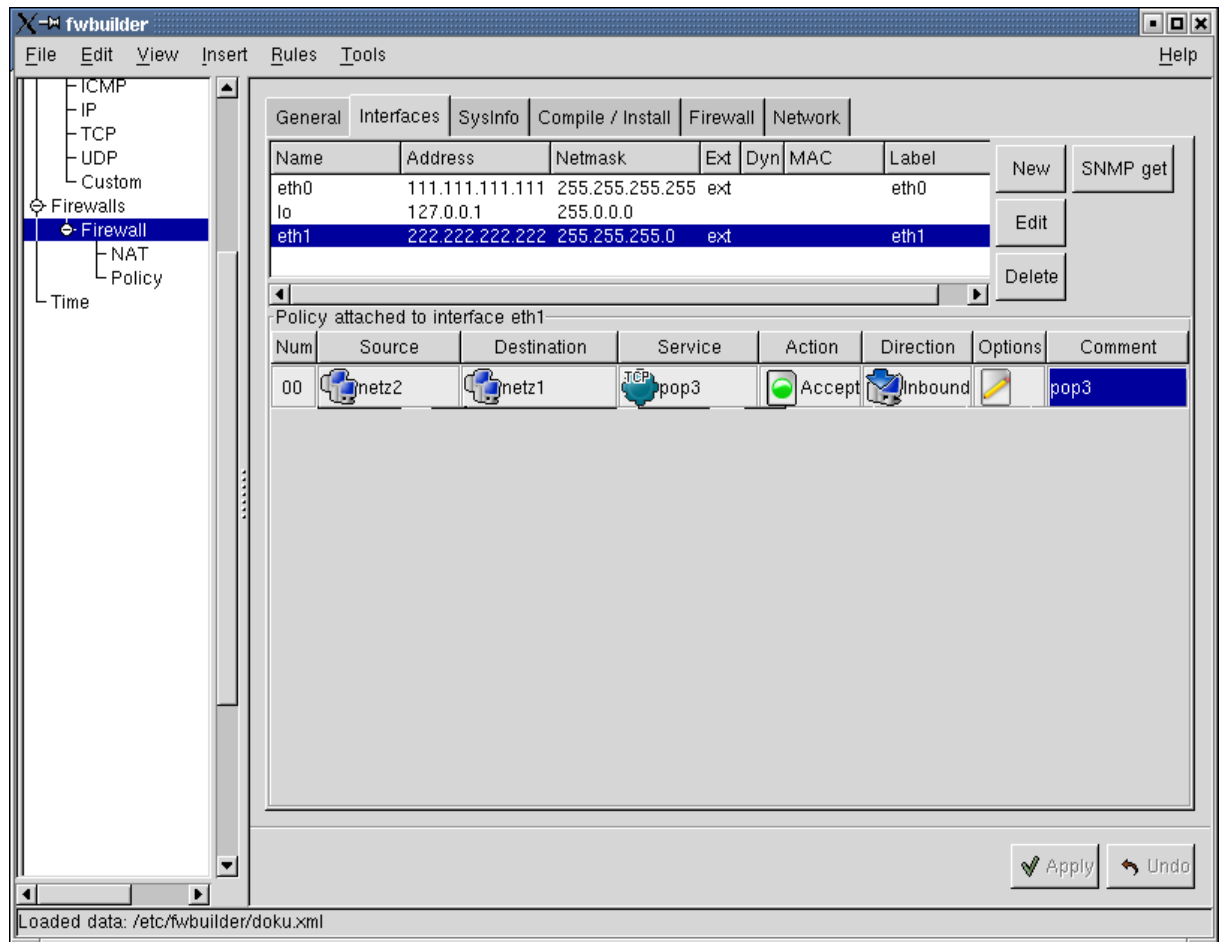


Abbildung 11-15: Eine fertig eingerichtete Regel für eth1

Für sämtlichen weiteren Regeln wiederholten sich die vorher aufgeführten Schritte bis die Regeln den Vorgaben die an die Firewall gestellt wurden erfüllt waren.

11.4.5 Globale Regeln

Abschließend werden nun noch die globalen Regeln nach dem selben Muster erstellt. Diese gelten nicht nur für einzelne Netzwerkschnittstellen sondern für die gesamte Firewall. Als letztes wird noch eine Regel angehängt, die alles verbietet was noch nicht erkannt wurde.

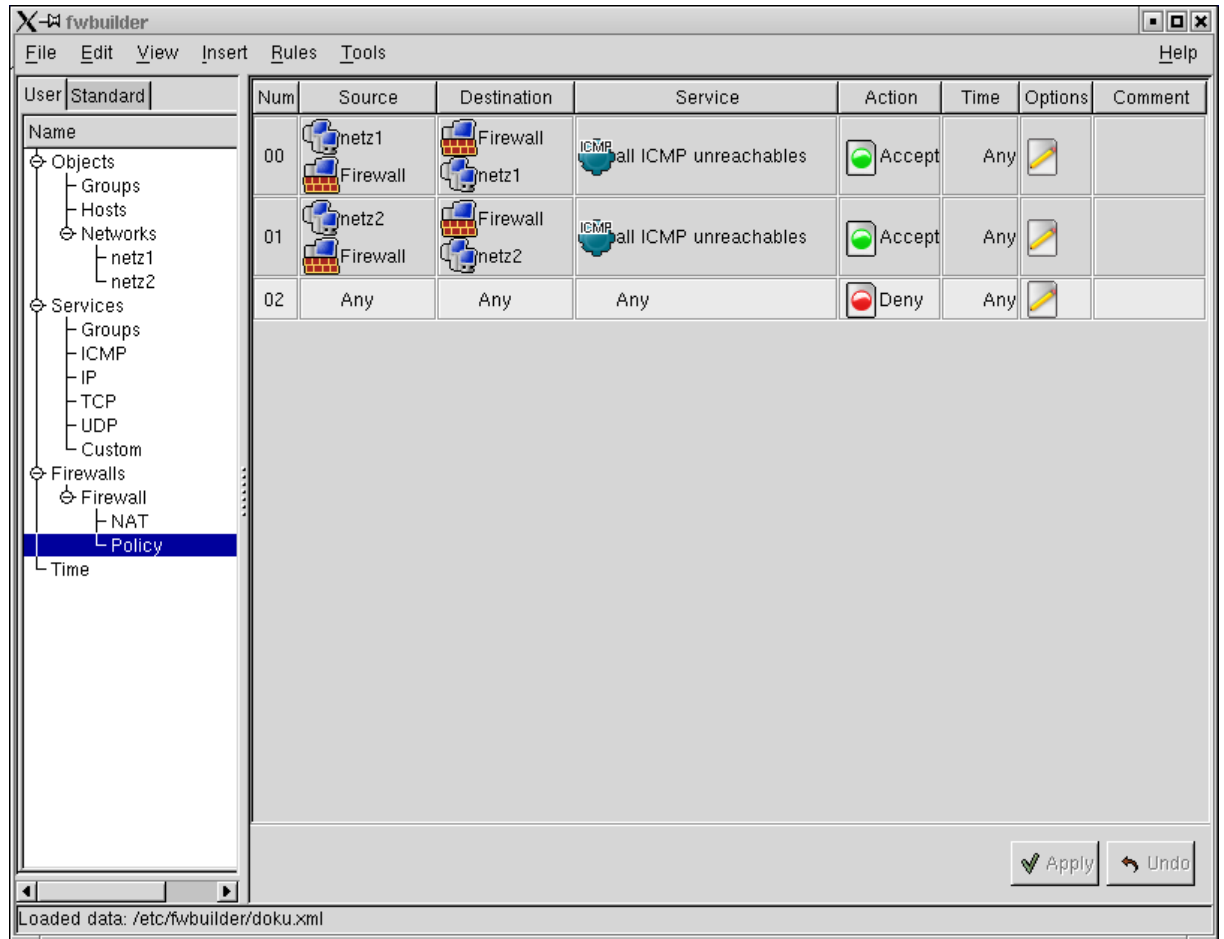


Abbildung 11-16: Globale Regeln für die Firewall

11.4.6 Firewall starten

Damit hatten wir die Konfiguration der Firewall abgeschlossen und speicherten sie ein letztes Mal ab. Anschließend wählten wir im Menü den Punkt <Rules>/<Compile> an. Firewall Builder generierte jetzt das Firewall-Skript und speichert es im Arbeitsverzeichnis `/etc/fwbuilder` ab. Von dort kann es über <Rules>/<Install> gestartet und anschließend ausgetestet werden.

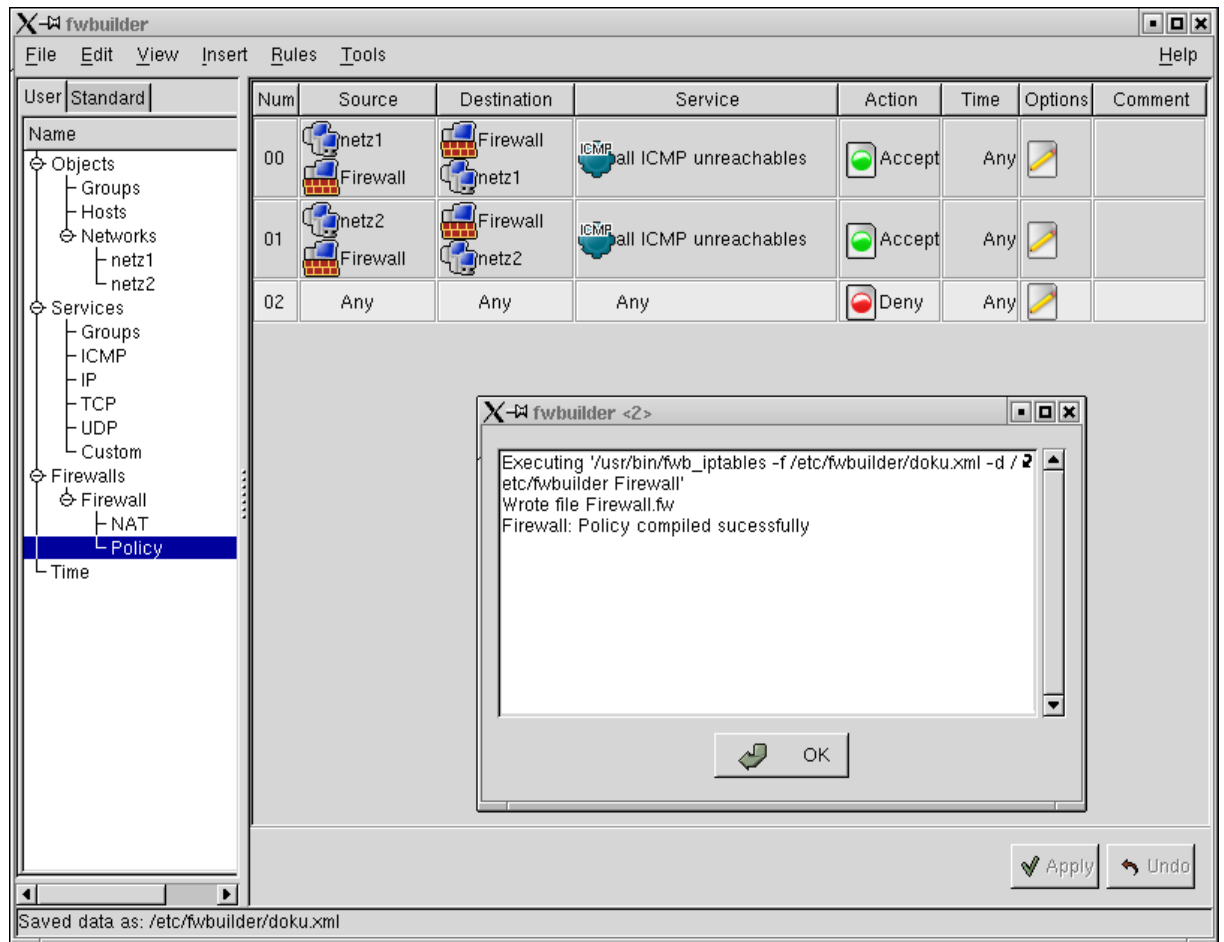


Abbildung 11-17: Meldung über die fertig kompilierte Firewall

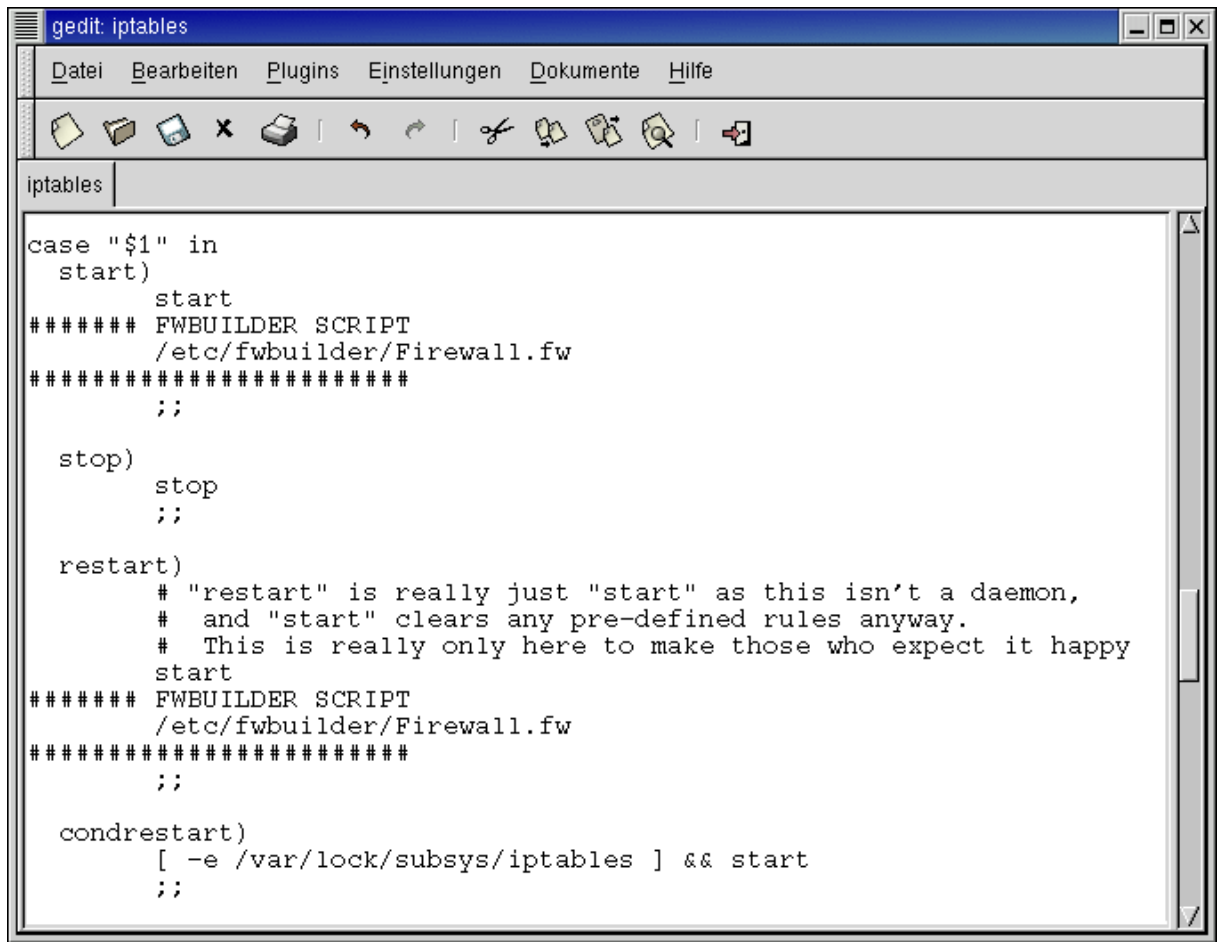


Abbildung 11-18: Automation des Firewallstarts

Um automatisch bei jedem Systemstart das aktuelle Firewall-Skript zu laden, trugen wir es in `/etc/init.d/iptables`, das Startup-Skript für Iptables, ein. Dazu suchten wir die Marken `start)` und `restart)` und ergänzten sie um den Befehl zur Ausführung der in `/etc/fwbuilder/` gespeicherten Regeln.

Eine Überprüfung unserer Firewall mit einem Portscanner wie z.B. `nmap` zeigte, dass unser Rechner durch nicht autorisierte Stationen tatsächlich nicht mehr entdeckt werden konnte. Potentiellen Angreifern bleibt er also künftig verborgen.

11.4.7 Abschluss- Betrachtung zum Firewall Builder

Die beschriebene Konfiguration reizt die Fähigkeiten des Firewall Builder bei weitem nicht aus. So lässt sich durch die Definition und Einbindung von Zeitspannen die Geltungsdauer von Regeln zeitlich beschränken. Daneben kann das Tool mehrere Firewall-Konfigurationen parallel vorhalten und bei Bedarf auf verschiedene Rechner verteilen. Viele dazu notwendigen Informationen holt sich Firewall Builder bei Bedarf per Knopfdruck via DNS und SNMP.

In jedem Fall reduziert Firewall Builder den Aufwand beim Erstellen, Austesten und Verteilen von Firewall-Policies drastisch, da die benötigten Regeln nicht von Hand in ein entsprechendes Script eingetragen werden müssen.

11.5 Erstelltes Script vom Firewall Builder

```
#!/bin/sh
#
# This is automatically generated file. DO NOT MODIFY !
#
# Firewall Builder fwb_iptables v1.0.0
#
# Generated Mon Apr 29 12:12:48 2002 CET by root
#
#
#

if [ -x /usr/bin/logger ]; then
  logger -p info "Activating firewall script Firewall.fw generated Mon Apr 29 12:12:48 2002 CET by root"
fi
modprobe ip_conntrack || exit 1
modprobe ip_conntrack_ftp || exit 1
modprobe ip_nat_ftp || exit 1

FWD=`cat /proc/sys/net/ipv4/ip_forward`
echo "0" > /proc/sys/net/ipv4/ip_forward

echo "30" > /proc/sys/net/ipv4/tcp_fin_timeout

echo "1800" > /proc/sys/net/ipv4/tcp_keepalive_intvl

iptables -P OUTPUT DROP
iptables -P INPUT DROP
iptables -P FORWARD DROP

cat /proc/net/ip_tables_names | while read table; do
  iptables -t $table -L -n | while read c chain rest; do
    if test "$c" = "XChain" ; then
      iptables -t $table -F $chain
    fi
  done
  iptables -t $table -X
done

ip addr flush dev eth0 scope link
ip addr flush dev lo scope link
ip addr flush dev eth1 scope link

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
#
# Interface Rule #0
#
# http
#
iptables -N IRULE_0_eth0
iptables -A INPUT -i eth0 -p tcp -m state --state NEW -s 111.111.111.111/255.255.255.0 --destination-port 80 -j
IRULE_0_eth0
iptables -A INPUT -o eth0 -p tcp -m state --state NEW -s 111.111.111.111/255.255.255.0 --destination-port 80 -j
IRULE_0_eth0
iptables -A IRULE_0_eth0 -j LOG --log-level info --log-prefix "RULE 0 -- Accept "
iptables -A IRULE_0_eth0 -j ACCEPT
#
# Interface Rule #0
#
# loopback
#
iptables -N IRULE_0_lo
iptables -A INPUT -i lo -m state --state NEW -j IRULE_0_lo
iptables -A OUTPUT -o lo -m state --state NEW -j IRULE_0_lo
iptables -A IRULE_0_lo -j LOG --log-level info --log-prefix "RULE 0 -- Accept "
iptables -A IRULE_0_lo -j ACCEPT
```

Fortsetzung auf der nächsten Seite

Fortsetzung

```
#
# Interface Rule #0
#
# pop3
#
iptables -N IRULE_0_eth1
iptables -A INPUT -i eth1 -p tcp -m state --state NEW -s 222.222.222.222/255.255.255.0 --destination-port 110 -j
IRULE_0_eth1
iptables -A IRULE_0_eth1 -j LOG --log-level info --log-prefix "RULE 0 -- Accept "
iptables -A IRULE_0_eth1 -j ACCEPT
#
# Rule #0
#
iptables -N RULE_0
iptables -A INPUT -p icmp -m state --state NEW -s 111.111.111.111/255.255.255.0 --icmp-type 3 -j RULE_0
iptables -A INPUT -p icmp -m state --state NEW -s 111.111.111.111 --icmp-type 3 -j RULE_0
iptables -A INPUT -p icmp -m state --state NEW -s 222.222.222.222 --icmp-type 3 -j RULE_0
iptables -A INPUT -p icmp -m state --state NEW -s 111.111.111.111 --icmp-type 3 -j RULE_0
iptables -A INPUT -p icmp -m state --state NEW -s 222.222.222.222 --icmp-type 3 -j RULE_0
iptables -A RULE_0 -j LOG --log-level info --log-prefix "RULE 0 -- Accept "
iptables -A RULE_0 -j ACCEPT
#
# Rule #1
#
iptables -N RULE_1
iptables -A INPUT -p icmp -m state --state NEW -s 222.222.222.222/255.255.255.0 --icmp-type 3 -j RULE_1
iptables -A FORWARD -p icmp -m state --state NEW -s 222.222.222.222/255.255.255.0 -d
222.222.222.222/255.255.255.0 --icmp-type 3 -j RULE_1
iptables -A INPUT -p icmp -m state --state NEW -s 111.111.111.111 --icmp-type 3 -j RULE_1
iptables -A INPUT -p icmp -m state --state NEW -s 222.222.222.222 --icmp-type 3 -j RULE_1
iptables -A INPUT -p icmp -m state --state NEW -s 111.111.111.111 --icmp-type 3 -j RULE_1
iptables -A INPUT -p icmp -m state --state NEW -s 222.222.222.222 --icmp-type 3 -j RULE_1
iptables -A OUTPUT -p icmp -m state --state NEW -d 222.222.222.222/255.255.255.0 --icmp-type 3 -j RULE_1
iptables -A RULE_1 -j LOG --log-level info --log-prefix "RULE 1 -- Accept "
iptables -A RULE_1 -j ACCEPT
#
# Rule #2
#
iptables -N RULE_2
iptables -A OUTPUT -m state --state NEW -j RULE_2
iptables -A INPUT -m state --state NEW -j RULE_2
iptables -A FORWARD -m state --state NEW -j RULE_2
iptables -A RULE_2 -j LOG --log-level info --log-prefix "RULE 2 -- Deny "
iptables -A RULE_2 -j DROP
#
# Final rules
#
iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
iptables -A FORWARD -j DROP

echo "$FWD" > /proc/sys/net/ipv4/ip_forward
```

12 Mailserver Sendmail

12.1 Allgemeines zu Sendmail

Einer der wichtigsten Services des Internet ist die elektronische Post. Für die Nutzung dieses Services ist sowohl das Senden als auch das Empfangen der Post einzeln zu konfigurieren.

Eric Allman schrieb hierfür ein Programm, namens Sendmail.

Sendmail ist ein multifunktionales Mailverteilsprogramm für Unix.

Man bezeichnet Sendmail als Mail-Transfer-Agent (MTA).

Gerade im Bereich bei den MTAs gibt es mehrere gute, konkurrierende Produkte.

Das noch immer am häufigsten verwendete Programmpaket ist allerdings Sendmail, da es bei vielen Distributionen schon auf den CD-ROMs enthalten ist.

Es sollte aber darauf geachtet werden, dass immer nur ein Mail Programm installiert ist, da es sonst zu Störungen kommen könnte. Bei der Installation des Linux RedHat 7.2 Betriebssystems wurde Sendmail automatisch mit eingebunden.

12.2 Funktion und Aufgaben eines Mailservers:

Unsere Aufgabe war es, den Mailserver so einzurichten, dass die Verwaltung und die Lehrer von ausgewählten Rechnern Mails senden und empfangen können.

Sendmail nimmt einerseits Emails von dem Mail User Agenten, mit anderen Worten ein Mailprogramm wie z.B. Outlook bei Microsoft, an und leitet diese Mail weiter.

Andererseits ist es ein Programm, dass ankommende Mails von anderen Mailservern entgegen nimmt und abspeichert, damit die User sich ihre Emails mit einem Mail User Agent (MUA) bei dem Mailserver abholen können. Der lokale Mailserver soll in regelmäßigen Abständen die Nachrichten zum Provider übermitteln und vom Provider abholen und lokal zustellen, d.h. im lokalen Postfach (Mailboxes) ablegen. Von den Arbeitsstationen im Netz werden dann die Mails vom lokalen Postfach abgeholt. Eine genauere Beschreibung des Mailverlaufs folgt auf den nächsten Seiten.

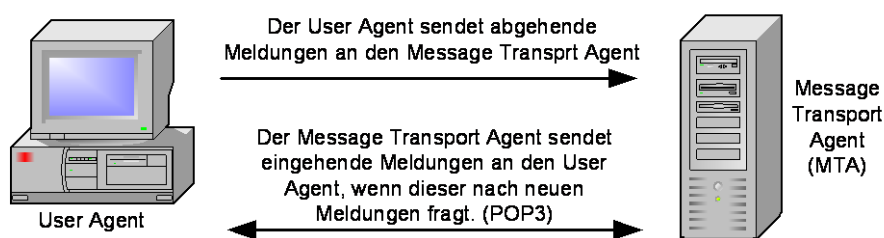


Abbildung 12-1: MTA und User Agent

12.3 Was ist überhaupt eine Mail ?

Ein elektronischer Brief besteht im allgemeinen zunächst aus dem Rumpf der Nachricht, also dem von Ihnen geschriebenen Text, und speziellen administrativen Daten, die die Empfänger angeben. Das Transportmedium usw. ist vergleichbar mit einem Briefumschlag.

Diese administrativen Daten lassen sich in zwei Kategorien einteilen. In die erste fallen alle Daten, die das Transportmedium betreffen, wie z.B. die Adresse des Absenders und Empfängers. Man spricht deshalb auch vom Briefumschlag, dem *Envelope*. Diese Daten können von der Transportsoftware transformiert werden, während sie die Botschaft weiterreicht.

Die zweite Kategorie umfasst alle Informationen, die zur Verarbeitung der E-Mail erforderlich sind und von jeglichem Transportmechanismus unabhängig sind. Dazu gehören beispielsweise die Betreff-Zeile (engl. *subject*), die Liste aller Empfänger, sowie Datum und Uhrzeit, wann die Botschaft abgeschickt wurde. In vielen Netzwerken hat es sich eingebürgert, diese Informationen der eigentlichen Botschaft als Briefkopf voranzustellen. Dieser Kopf (oder *mail header*) ist vom Rumpf (oder *mail body*) der Botschaft durch eine Leerzeile getrennt.

Die meisten Mail-Programme in der UNIX-Welt verwenden ein Header-Format, das in RFC-822 skizziert ist. Sein ursprünglicher Zweck war es, einen Standard für das ARPANET zu schaffen. Da es so entworfen wurde, dass es unabhängig von irgendeiner bestimmten Netzwerkumgebung ist, wurde es auch leicht an andere Netze angepasst, einschließlich vieler UUCP-basierter Netze.

RFC-822 ist allerdings nur der größte gemeinsame Nenner. In jüngerer Zeit sind verschiedene Standards entwickelt worden, die den wachsenden Bedarf an Zusätzen, wie Verschlüsselung, Unterstützung für internationale Zeichensätze und MIME (Multipurpose Internet Mail Extensions, bewältigen sollen.

All diese Standards gehen davon aus, dass ein Mail-Header aus mehreren Zeilen besteht, getrennt durch Zeilenendezeichen. Eine Zeile setzt sich jeweils aus einem Feldnamen zusammen, der in Spalte eins beginnt, und dem Feld selbst, das durch einen Doppelpunkt und ein Leerzeichen abgesetzt ist. Das Format und die Bedeutung der einzelnen Felder variiert in Abhängigkeit vom Feldnamen. Ein Header-Feld kann über eine Zeile fortgesetzt werden, wenn die nächste Zeile mit Leerzeichen (Blank oder TAB) beginnt. Die Reihenfolge der Felder spielt keine Rolle.

Für den normalen User ist meist nur folgender Header von Interesse:

- Die To- Zeile: Hier erscheint der Adressat der Nachricht.
- Die From- Zeile: Hier steht der Absender der Mail drin.
- Die Cc- Zeile: Cc steht für Carbon copy, was wörtlich Durchschlag bedeutet, Adressaten, die in der Cc- Zeile stehen, erhalten eine Kopie dieser Mail
- Die Bcc- Zeile: Bcc heißt Blind carbon copy und bedeutet, dass es sich um eine „versteckte“ Kopie der Mail handelt.
- Subject: Das ist der Betreff der Nachricht.⁷



Abbildung 12-2: Mail Verlauf über einen Server

12.4 Die Datei Sendmail.cf

Es gibt viele unterschiedliche Konfigurationstools, die im Endeffekt allerdings immer zum selben Ziel führen, nämlich zum Einrichten bestimmter Dateien. Im Fall von Sendmail sind es diese Dateien:

`/etc/sendmail.cf`

und die Dateien im Verzeichnis `/etc/mail/`.

Da die Datei `/etc/sendmail.cf` allerdings die größte und umfassendste Datei auf dem Linux Betriebssystem ist und zusätzlich noch eine eigene Syntax hat, ist von einer Änderung hier auf jeden Fall abzuraten.

Zu fast allen Einstellungen, die wir zu dem Projektteil „Mailserver Sendmail“ gemacht haben, benutzten wir das Konfigurationstool Webmin, welches auf die gerade erwähnten Dateien zugreift, dabei aber ein übersichtliches, verständliches Werkzeug für den Administrator bietet. Ein paar andere Einstellungen wurden über die Konsole gemacht, wobei diese im folgenden Teil noch genau beschrieben werden. Alle Dateien, lassen sich auch über die shell bearbeiten. In der nun folgenden Beschreibung sind die Dateien **Fett gedruckt**, die Änderungen mit Webmin sind *kursiv geschrieben*. Andere Einstellungen, wie z.B. unter Windows, sind unterstrichen. Bei den direkten Dateiänderungen auf der shell sind Datenbank-Versionen von den jeweiligen Konfigurationsdateien zu erstellen, weil Sendmail schneller auf diese zugreifen kann. Diese DBM-Datenbanken werden mit dem Befehl:

```
makemap hash /etc/mail/configdatei < /etc/mail/configdatei
```

gemacht. Es gibt aber auch hier eine Ausnahme, nämlich die `/etc/mail/aliases` Datei, welche mit dem Befehl `newalias` zu einer Datenbankdatei wird.

Wie bereits erläutert, haben wir die Änderungen weitestgehend mit Webmin vorgenommen, aber für einen versierten Administrator ist diese Art der Shell-Einstellung auch allein aus zeittechnischen Gründen sehr interessant.

`/var/named/named.BBS2`

Der MX-Record leitet Mails an einen Mailserver weiter. Hierbei kann die Mail für einen einzelnen Rechner oder für eine vollständige Domain weitergeben werden. Es muss für den Mailserver ein MX (Mail-Exchange-Records) Eintrag festgelegt werden, um SMTP –Mailserver Ressourcen in einer Domain zu kennzeichnen. In unserem Fall muss dem Eintrag

```
IN MX 5 mail.bbs2.fh-wilhelmshaven.de
```

und

```
IN MX 50rz5.rz-wilhelmshaven.de
```

sein.

Es ist auch möglich, mehrere MX Einträge zu haben, wobei der Präferenzwert (5) eine wesentliche Rolle spielt. In diesem Fall wird die Mail erst vom BBS Mailserver versendet und dann vom FH Mailserver. Bei mehreren Mailservern wird dann die Mail mit dem Server, der die kleinste Nummer hat (größte Priorität) zuerst versendet.

12.5 POP 3 Dienst aktivieren

Shell: `/etc/xinetd.conf` (Extended Internet Service Daemon Konfigurationsdatei)
Diese Datei bezieht den Ordner `/etc/xinetd.d` mit ein. Hier sind die einzelnen Dienste in eigene Dateien verteilt.

In der Datei `/etc/xinetd.d/ipop3` muss der pop3 Service frei geschaltet werden.

```
# default: off
# description:
# The POP3 service allows remote users to access their mail \
# using a POP3 client such as Netscape Communicator, mutt, \
# or fetchmail.

service pop3
{
    socket_type      = stream
    wait            = no
    user             = root
    server           = /usr/sbin/ipop3d
    log_on_success   += USERID
    log_on_failure   += USERID
    disable          = no<- hier wird der Dienst aktiviert(no statt yes)
}
```

Danach musste der xinetd.d Dienst neu gestartet werden, was wir mit dem Befehl

```
/etc/init.d/xinetd.d restart
```

erreicht haben.

Der Mailserver Sendmail wird als eigenständiger Prozess gestartet und nicht über den xinetd verwaltet. Sendmail startet man mit

```
/usr/sbin/sendmail -q
```

(-q = Warteschlangenbearbeitungsintervall)

Sendmail stoppen:

```
/etc/rc.d/init.d/sendmail stop
```

Um Sendmail zu starten:

```
/etc/rc.d/init.d/sendmail start
```

Tipp zum deaktivieren von Diensten:

Deaktivieren Sie Dienste nur über das Setzen von Kommentarzeichen (#), nicht durch löschen der Zeile. Wenn später der Dienst doch wieder gebraucht wird, dann kann er leicht wieder aktiviert werden, indem einfach das Kommentarzeichen weggenommen wird.

12.6 Konfiguration mit Webmin

[Webmin Index](#)
[Modul Index](#)

Sendmail-Einstellungen

[Zurück zu Sendmail-Konfiguration](#)

Abbildung 12-3: Sendmail Einstellungen

Diese Einstellungen werden direkt in die Sendmail.cf Datei geschrieben, wichtig hierbei ist der Eintrag „SMTP port options“. Dort werden die Ports eingetragen, auf die der SMTP Dämon „hört“. Und zwar, der Port mit der Adresse 139.13.210.1 für alle lokalen Emails und der Port 139.13.223.18 für alle Emails die aus dem Internet kommen. Außerdem kann hier auch ein Smarthost unter „Sende ausgehende Mail durch Host“ eingetragen werden.

Smarthost

Dies ist einfach der Rechner, an den diejenige Post geschickt wird, die nicht lokal zugestellt werden kann. Lokal zustellen heißt, dass Post von einem Benutzer des Linux

Systems an einen anderen Benutzer des gleichen Systems geschickt wird. Stellt Sendmail fest, dass es sich um einen Benutzer außerhalb des Systems handelt, übergibt es die Post einfach an den Smarthost. Es ist derjenige Server, der die Sprache SMTP versteht. Man kann den Smarthost direkt in der Sendmail.cf Datei eintragen unter „Smart“ relay host (may be null) oder mit Webmin unter

Server->Sendmail->Sendmail Einstellungen-> Sende ausgehende Mail durch host

Der Vorteil durch diesen Eintrag sind bessere Geschwindigkeiten innerhalb des Systems, da bei lokalen Mails nicht versucht wird, sie über das Internet zu verschicken. Eine weitere sinnvolle Anwendung für Smarthost Konfigurationen ist die Transportverwaltung von Mail über private Firewalls. Bei unserem Netzwerk sind die eigenen unregistrierten IP Adressen von einer Firewall geschützt. Wollte man nun Mails von den Hosts des Schulnetzwerkes mittels SMTP an die Außenwelt senden oder empfangen, wäre das mit einer konventionellen Konfiguration nicht zu machen. Die Hosts wären nicht in der Lage, eine direkte Netzwerkverbindung zum Internet herzustellen. Die Lösung hierfür ist den Firewall-Rechner auch als Smart Host für die Mailverwaltung agieren zu lassen.

Der Smart Host würde Mails von beiden Seiten annehmen, im lokalen Speicher ablegen und dann für die erneute Übertragung der Mails an die gewünschten Hosts sorgen.

12.6.1 Benutzer und Gruppen

Webmin: System → Benutzer und Gruppen
Shell: /etc/passwd

Als nächstes wurden Benutzer und Gruppen hinzugefügt. Dieses ist genau wie die beiden nächsten Einstellungen eine Sache, die immer aktualisiert werden muss. Deshalb haben wir die erforderlichen Einstellungen ganz ausführlich in dem Benutzerhandbuch beschrieben.

[Webmin Index](#)
[Hilfe](#)
[Modul-Konfiguration](#)

Benutzer und Gruppen

[Suche in der Hilfe](#)

Lokale Benutzer

Benutzername	Benutzer-ID	Wirklicher Name	Stammverzeichnis	Shell
adm	3	adm	/var/adm	/sbin/nologin
amanda	33	Amanda user	/var/lib/amanda	/bin/bash
xfs	43	X Font Server	/etc/X11/fs	/bin/false

[Neuen Benutzer hinzufügen](#)

Lokale Gruppen

Gruppenname	Gruppen-ID	Mitglieder
adm	4	root adm daemon
apache	48	
bin	1	root bin daemon
users	100	sopp berber biern boesa ebeling ewendi fiedler gerdes hansen jech johan kloetz lange schollb seibt steffen szkodow troeck wagner welle wengerow woeste wendisch fpelektro fpbauholz steinro mucha linnem siegert jan tsbs
utmp	22	
uucp	14	uucp
wagner	518	
welle	519	
wendisch	522	
wengerow	520	
wheel	10	root
wine	101	
woeste	521	
xfs	43	

[Neue Gruppe erstellen](#)

Zeige Anmeldungen für

Logged In Users

[← Zurück zu Startseite](#)

Abbildung 12-4: Benutzer und Gruppen

Hier gibt es einen Überblick auf alle Benutzer, die schon eingetragen sind. Änderungen kann man bei jedem einzelnen durch anklicken des Namens vornehmen.

Nachdem man unter Benutzer und Gruppen „Neuen Benutzer hinzufügen“ gedrückt hat, erscheint folgendes Bild. Hier wird dann ein neuer Benutzer Account angelegt.

[Webmin Index](#)
[Modul Index](#)
[Hilfe..](#)

Benutzer anlegen

Benutzerdetails			
Benutzername	lehrer	Benutzer-ID	536
Wirklicher Name	Lehrer	Stammverzeichnis	/home/lehrer ...
Shell	/bin/sh ▾	Kennwort	☐ Kein Kennwort benötigt ☐ Keine Anmeldung erlaubt ☐ Klartextkennwort ☒ Vorverschlüsseltes Kennwort JKmXtGuOfS
Andere..	...		

Kennworteinstellungen			
Kennwort geändert	Niemals	Ablaufdatum	Jan / / ...
Minimale Anzahl von Tagen		Maximale Anzahl von Tagen	
Warnung nach Tagen		Inaktive Tage	

Gruppenzugehörigkeit	
Primäre Gruppe ☐ Neue Gruppe lehrer ... ☒ Existierende Gruppe users ...	Sekundäre Gruppe adm (4) apache (48) bin (1) daemon (2) dip (40)

Beim Erstellen..	
Erstelle Stammverzeichnis?	☒ Ja ☐ Nein
Kopiere Dateien zu Stammverzeichnis?	☒ Ja ☐ Nein
Create user in other modules?	☒ Ja ☐ Nein

Erstellen

← [Zurück zu Benutzer- und Gruppenliste](#)

Abbildung 12-5: Benutzer anlegen

12.6.2 Spam-Kontrolle (access, Shell: /etc/mail/access)

[Webmin Index](#)
[Modul Index](#)

Spam-Kontrolle

Spam-Kontrollregel erstellen

Mail-Quelle:

☒ Akzeptieren ☐ Erlaube Weiterleitung
☐ Abweisen ☐ Leise löschen
☐ Fehlercode: Nachricht:

Quelle..	Aktion..
localhost.localdomain	RELAY
localhost	RELAY
127.0.0.1	RELAY
139.13.210.1	RELAY
139.13.223.18	RELAY

139.13.210.158	DENY
139.13.210.159	DENY

139.13.210.160	DENY
139.13.210.161	DENY
139.13.210.162	DENY
139.13.210.163	DENY
139.13.210.164	DENY

139.13.210.253	DENY
139.13.210.254	DENY

[/etc/mail/access manuell bearbeiten](#)

Sendmails Spam-Kontrolle ermöglicht es Ihnen, Ihr System vor Spam zu schützen, indem E-Mails von bestimmten Adressen abgewiesen werden. Ebenso verhindert es, dass Spammer Ihr System zum Weiterleiten von Spam benutzen. Standardmäßig akzeptiert Sendmail alle E-Mails für lokale Benutzer, verweigert jedoch allen Clients oder Mailservern, E-Mail über Ihr System weiterzuleiten. Typischerweise werden Sie Anti-Spam-Regeln hinzufügen, um E-Mails von Spammern abzuweisen, und Regeln, um anderen Maschinen auf ihrem Netz das Weiterleiten von E-Mail über Ihr System zu gestatten.

← [Zurück zu Sendmail-Konfiguration](#)

Abbildung 12-6: Spam Kontrolle

Um Missbrauch von dem Mailserver zu verhindern, wurden nur bestimmte Rechner für das Versenden und Empfangen von Email bestimmt. Das so genannte Spamming wurde durch den Eintrag in die Datei `/etc/access.db` für alle anderen Rechner unterbunden. SPAM ist die landläufige Bezeichnung für kommerzielle Werbemails (UCE bzw. UBE für "unsolicited commercial/bulk e-mail", für Kettenbriefe ("chain letter"), für MMF-Systeme ("Make Money Fast") und ähnliche unerwünschte Mails oder Postings in News-Gruppen.

Das Bild zeigt deutlich, wie Spammer einen Mailserver ausnutzen können, um zum Beispiel Werbemails zu versenden. Die Funktion ist ähnlich wie bei den so genannten „Kettenbriefen“, die auf dem normalen Postweg verschickt werden. Wir haben unter Webmin alle Rechner der Schule eingetragen, aber nur bestimmten Hosts erlaubt, von ihnen aus Emails zu senden und zu empfangen. Somit ist gewährleistet, dass kein Schüler Emails über den Server verschicken kann.



12.6.3 Mail Aliases (Shell: `/etc/mail/aliases`)

[Webmin Index](#)
[Modul Index](#)
[Hilfe..](#)

Mail-Aliases

Alias erstellen

Adresse

Aktiviert? ☒ Ja ☐ Nein

Alias zu

Adresse	Alias auf..
mailer-daemon	Adresse postmaster
postmaster	Adresse linnem
bin	Adresse root
daemon	Adresse root
adm	Adresse root
lp	Adresse root
sync	Adresse root
shutdown	Adresse root
halt	Adresse root
mail	Adresse root
news	Adresse root
uucp	Adresse root
operator	Adresse root
games	Adresse root
gopher	Adresse root
ftp	Adresse root
nobody	Adresse root
apache	Adresse root
named	Adresse root
xfs	Adresse root
gdm	Adresse root
mailnull	Adresse root
postgres	Adresse root
squid	Adresse root
rpcuser	Adresse root
rpc	Adresse root

Adresse	Alias auf..
ingres	Adresse root
system	Adresse root
toor	Adresse root
manager	Adresse root
dumper	Adresse root
abuse	Adresse root
newsadm	Adresse news
newsadmin	Adresse news
usenet	Adresse news
ftpadm	Adresse ftp
ftpadmin	Adresse ftp
ftp-adm	Adresse ftp
ftp-admin	Adresse ftp
decode	Adresse root
root	Adresse marc Adresse mailman Adresse aliases
mailman	Adresse postmaster
mailman-owner	Adresse mailman
verwaltung	Adresse sopp
E.Sopp	Adresse sopp
U.Schollenberger	Adresse schollb
Beckmann Eilts	Adresse beckeilt
P.Johannsen	Adresse johan
I.Wendisch	Adresse wendisch

[/etc/aliases manuell bearbeiten](#)

← [Zurück zu Sendmail-Konfiguration](#)

Mail-Aliases ist die dritte Datei, die vom Administrator immer beobachtet werden muss. Hierfür steht eine ausführliche Beschreibung in dem Benutzerhandbuch. Wichtig sind Eintragungen bei Namensänderungen, bei neuen Usern die hinzugeführt werden, aber

auch wenn z.B. ein Administratorwechsel vorgenommen wird. Diese Datei umschreibt die Usernamen in die richtigen Namen und mit dieser Datei kann man eine Emailadresse mehreren Postfächern zuordnen, wie es beim root der Fall ist.

Die nun folgenden Einstellungen sind nur einmal zu bewerkstelligen, können aber bei Erweiterung des Systems noch verändert werden.

12.6.4 Domänenverknüpfung (domaintable, Shell: /etc/mail/domaintable)

Wenn z.B. der Domainname geändert werden soll, kann jenes mit diesem Filter geschehen, indem man den Namen bei ein- und ausgehenden Emails einfach austauscht. Dies funktioniert sogar, wenn User noch den alten Domainnamen in ihrem Mailprogramm eingetragen haben.

Dieses Feature ist bei dem Mailserver der BBS2 aber nicht aktiviert da es wohl nicht zu einer Änderung des Domainnamens kommen wird. Wichtig wäre es zum Beispiel bei einer Änderung, bei der alle User erhalten bleiben sollen. Dies erspart viel Zeit durch eine ausbleibende Neukonfiguration.

12.6.5 Domänen-Routing (mailertable, Shell: /etc/mail/mailertable)

Mailertabellen sind eine einfache Möglichkeit, Nachrichten anhand von Rechner- und Domainnamen an unterschiedliche Delivery- Agenten zu leiten.

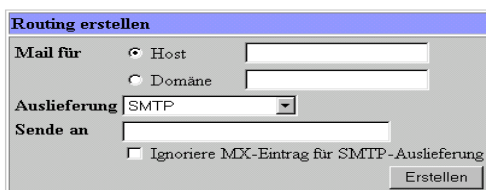
Man kann also auch noch einen „mailertable“ definieren. Mit dieser Datei kann der Transport zu bestimmten (1) Smarthosts delegiert werden. Außerdem können beispielsweise Mails an „domain.com“ über den Smarthost „provider.de“ verschickt und gleichzeitig alle anderen Mails an fh-wilhelmshaven.de zugestellt werden.

Diese Datei wird vor allem daher notwendig, weil zunehmend Mailserver im Internet gegen Relaying dicht gemacht werden (um so die Rechner als Ausgangspunkt von Spam noch besser zu schützen) und um das Zustellen nur noch von bestimmten anderen Hosts aus zuzulassen.

Zu beachten ist hier die Reihenfolge der Einträge. Der erste, von oben nach unten, passende Eintrag wird genommen. Der letzte Eintrag gilt dann für alle Mails, die nicht schon vorher ausgewählt wurden.

[Webmin Index](#)
[Modul Index](#)

Domänen-Routing



[/etc/mail/mailertable manuell bearbeiten](#)

Domänen-Routing stellt eine Methode zur Verfügung, um eine spezielle Transfermethode für bestimmte Domänen festzulegen. Dies kann nützlich sein, wenn Ihr System ein Gateway für Mailserver ist, die nicht von außerhalb Ihres Netzwerks erreichbar sind, oder wenn Sie alle E-Mails für eine bestimmte Domäne über einen anderen Server leiten wollen.

Sie sollten für eine geroutete Domäne **keinen** Eintrag in der Liste [lokalen Domänen](#) haben. Sie sollten aber für alle Domänen, für die dieses Gateway zuständig ist, einen DNS-MX-Eintrag haben, der auf Ihr System zeigt.

← [Zurück zu Sendmail-Konfiguration](#)

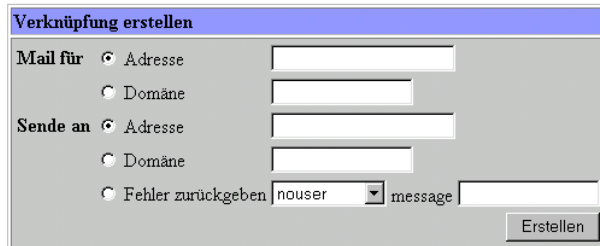
Abbildung 12-7: Domänen Routing

12.6.6 Adressenverknüpfung (virtuser, /etc/mail/virtusertable)

Sendmail verwendet diese, um bei entgegengenommenen Mails die offiziellen Adressen wieder in lokale umzusetzen. Dieses ist aber erst sinnvoll, bei mehreren Domains.

[Webmin Index](#)
[Modul Index](#)

Adressenverknüpfung



[/etc/mail/virtusertable manuell bearbeiten](#)

Adressenverknüpfungen sind vergleichbar mit [Aliases](#), aber sie sind besser geeignet für Systeme, die mehrere E-Mail-Domänen behandeln. Sie können benutzt werden, um ganze Domänen zu einer einzigen Adresse umzuleiten, um Benutzer mit einem Namen in mehreren Domänen zu behandeln oder um alle E-Mails zu einer Domäne zu einer anderen umzuleiten.

Beachten Sie, dass Sie einen Eintrag in der Tabelle für [lokale Domänen](#) für alle Domänen haben müssen, für die Adressenverknüpfung benutzt wird. Ebenso muss im DNS-Eintrag für jede Domäne ein MX-Eintrag vorhanden sein, der auf Ihr System verweist.

← [Zurück zu Sendmail-Konfiguration](#)

Abbildung 12-8: Adressenverknüpfung

12.6.7 Ausgehende Adressen (generics, /etc/mail/genericstable)

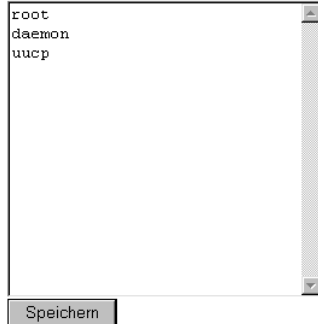
Genericstable ist für die Umsetzung der lokalen Namen in offizielle, im Internet gültige Namen zuständig, bzw. lässt sich dazu verwenden. Es wird einfach zu jeder lokalen Email-Adresse eine passende „für draußen“ definiert. Genericstable lädt Regeln, mit denen man Senderadressen ändern kann, wenn der Sender auf andere Rechner umgezogen ist. Dieses Feature ist nicht beim Mailserver aktiviert.

12.6.8 Vertraute Benutzer

[Webmin Index](#)
[Modul Index](#)

Vertraute Benutzer

Lokale Benutzer, denen von Sendmail getraut wird



```
root
daemon
uuwp
```

Speichern

Wenn ein lokaler Benutzer versucht E-Mails zu versenden, wird Sendmail ihm nur gestatten eine andere Adresse unter From: anzugeben, wenn er in der Liste links steht. Diese Einschränkung hält Benutzer davon ab, gefälschte From:-Adressen in E-Mails zu benutzen, die von Ihrem System aus gesendet werden.

 [Zurück zu Sendmail-Konfiguration](#)

Abbildung 12-9: Vertraute Benutzer

Im Normalfall haben alle User der Schule folgende Absenderadresse:

User@bbs2.fh-wilhelmshaven.de

Unter dem Punkt „Vertraute Benutzer“ werden die Namen der User eingetragen, die auch mit einer anderen Absenderadresse Emails aus dem Netzwerk versenden dürfen.

12.6.9 Weiterleitungsdomänen

[Webmin Index](#)
[Modul Index](#)

Weiterleitungsdomänen

Domänen, zu denen Weiterleitung gestattet ist.

bbs2.fh-wilhelmshaven.de
fh-wilhelmshaven.de

Speichern

Wenn es nicht durch eine [Spam-Kontrollregel](#) erlaubt ist, wird Sendmail das Weiterleiten nur von Domänen gestatten, die links aufgelistet sind. Eingehende Mail, die nicht für einen lokalen Benutzer und nicht für eine hier angegebene Domäne sind, werden abgewiesen.

Wenn Ihr System als Gateway für mehrere Domänen arbeitet, die nicht direkt (durch Benutzen der [Domänen-Routing](#)-Funktion), von außerhalb des Netzwerks zu erreichen sind, sollten alle solche Domänen hier aufgelistet sein.

← [Zurück zu Sendmail-Konfiguration](#)

Abbildung 12-10: Weiterleitungsdomänen

Wenn die Meldung: „We do not Relay“ ankommt, muss eine Liste erstellt werden, in der alle

Domains eingetragen werden, an die Email gesendet werden darf. Also die Zieldomain, da es nun aber unendlich viele Domains gibt, wird hier nur die Endung eingetragen.

Bei allen Domains für Deutschland ist es dann: .de

Für alle anderen Domains sind es dann zum Beispiel: .com, .org usw.

12.6.10 Domänenmaskierung

Dieses Feature veranlasst, dass alle ausgehenden Adressen so transformiert werden, als ob sie von der angegebenen Domain kämen.

Da es in unserem Fall aber nur eine Domäne gibt, ist hier nur ein Eintrag vorhanden.

[Webmin Index](#)
[Modul Index](#)

Domänenmaskierung

Maskiere als Domäne

Domänen, die maskiert werden sollen

Falls eine Domäne oben angegeben ist, wird Sendmail die Absenderadresse (From-) für alle ausgehenden E-Mails so ändern, als würden Sie von dieser Domäne kommen. Zusätzlich werden die Absenderadressen (From-) von E-Mails, die durch Ihr System transferiert werden, von einer der Domänen, die links angegeben sind, auf die gleiche Weise geändert. Beachten Sie, dass jede Domänenmaskierung für einzelne Benutzer durch die Seite "[Ausgehende Adressen](#)" überschrieben werden kann.

Diese Funktion kann nützlich sein, wenn ausgehende E-Mails von Ihrem Domännennamen und nicht von ihrem Host-Namen kommen soll oder wenn Ihr System ein Mailverteiler für eine Reihe anderer Hosts ist, die Ihre eigenen Mailserver betreiben.

 [Zurück zu Sendmail-Konfiguration](#)

Abbildung 12-11: Domänenmaskierung

12.7 Smtppop-E-Mail-Clients einrichten

Dies ist die Schnittstelle zwischen dem Mailserver und den Benutzern. Bei diesem Server werden wohl die meisten Benutzer ihre Post auf Windows-Maschinen mit einem POP3-Client lesen. Um es ihnen zu ermöglichen einen typischen POP3/SMTP Mailclient zu konfigurieren, müssen jedem Benutzer folgende Informationen mitgeteilt werden.

Als Beispiel:

SMTP-Server (SMTP=Simple Mail Transfer Protocol)	SMTP.bbs2.fh-wilhelmshaven.de
POP3-Server (Post Office Protocol Version 3) zum Abholen von E-Mails die beim Provider in einer Art Briefkasten zwischengespeichert wurden.	Mail. bbs2.fh-wilhelmshaven.de
E-Mail-Adresse muss weltweit eindeutig sein, oft mit folgendem Aufbau: Vorname.Nachname@provider.de wobei 'de' hier die Landkennung für Deutschland ist	tester@ bbs2.fh-wilhelmshaven.de
Benutzerkennung	Tester
Passwort nur mit Benutzerkennung und passendem Passwort kann die E-Mail abgeholt werden	mlddik97

Ein Mail-Client erlaubt dann:

- Empfangen (Zugriff auf die Mailbox)
- Bearbeiten
- Verwalten
- Versenden einer Mail

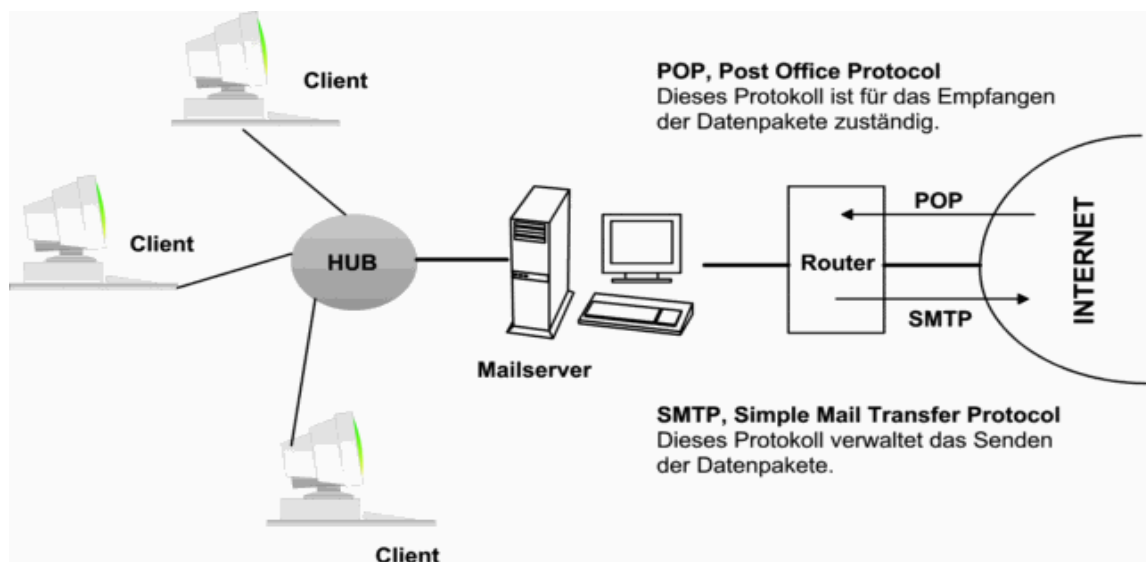
12.8 Wie Mail Transportiert wird

Für gewöhnlich werden Sie Ihre E-Mails mit Hilfe von Programmen wie Outlook(Microsoft) oder *Kmail* (Linux)schreiben.. Diese Programme werden im Englischen als *Mail User Agents* bezeichnet (*agent* heißt Werkzeug) und MUA abgekürzt. Wenn Sie eine Nachricht abschicken, wird sie von Ihrem Benutzerprogramm in der Regel an ein anderes Programm weitergereicht, das den Transport zum Zielsystem übernimmt. Dieses Programm heißt *Mail Transport Agent*, kurz MTA. Auf den meisten Systemen wird derselbe MTA sowohl für lokalen als auch fernen Versand benutzt — in der Regel `/usr/sbin/sendmail`.

Die Auslieferung einer Mail an einen lokalen Benutzer umfasst natürlich mehr, als sie nur an die Mailbox-Datei des Benutzers anzuhängen. Für gewöhnlich muß sich der

lokale MTA um Aliasing (Einrichtung lokaler Empfänger-Adressen, die auf andere Adressen verweisen) und Forwarding (Umleiten einer Benutzer-Mail auf ein anderes Ziel) kümmern. Außerdem müssen nicht zustellbare Mails mitsamt einem Fehlerreport an den Absender zurückgesandt werden; im Englischen wird dieser Vorgang als *bouncing* bezeichnet. Bei der Auslieferung über ein anderes System hängt es ganz von der Art der Netzverbindung ab, welche Transportsoftware verwendet wird. Werden die Nachrichten über ein TCP/IP basiertes Netz zugestellt, wird für gewöhnlich SMTP verwendet. SMTP steht für *Simple Mail Transfer Protocol* und ist in RFC-821 beschrieben. SMTP wurde so entworfen, dass eine Nachricht direkt an eine Empfänger-Maschine zugestellt wird, wobei die Nachrichtenübertragung mit dem SMTP Dämon der Gegenseite ausgehandelt wird. In Unternehmen ist es heutzutage üblich, spezielle Hosts (Smarthosts) zur Verfügung zu stellen, die alle an Empfänger im Unternehmen gerichteten Mails aufnehmen und ordnungsgemäß an die gewünschten Empfänger weiterleiten.

POP3 (Post Office Protocol Version 3) ist die aktuelle Version des Protokolls zur Übertragung von Emails zwischen dem Mail Server und dem lokalen Rechner.



12.9 Mail-Routing im Internet

Im Internet ist es ganz vom Zielsystem abhängig, ob überhaupt ein besonderes Mail-Routing vorgenommen wird. Im Normalfall wird eine Nachricht direkt an den Zielrechner übertragen, wobei zuerst festgestellt wird, an welchen Host die Nachricht gesendet werden soll, und danach die Nachricht direkt an diesen Host zugestellt wird. Die meisten Internet-Sites werden es allerdings vorziehen, dass alle eingehenden Mails von einem zentral verfügbaren Server entgegengenommen und lokal verteilt werden. Um diesen Dienst bekannt zu machen, veröffentlicht die Site im DNS einen sogenannten MX-Record für ihre lokale Domain. MX steht für den englischen Terminus *Mail Exchanger*. Im Grunde besagt ein MX-Record, dass der Server-Host bereit ist, alle Mail-Adressen in der Domain anzunehmen und weiterzuleiten. MX-Records können auch dazu verwendet werden, den Datenverkehr von Hosts, die nicht selbst ans Internet angeschlossen sind, zu verwalten. Typische Beispiele sind UUCP-Netzwerke und FidoNet-Rechner, deren Mails durch ein Gateway geleitet werden müssen. Einem MX-Record ist immer eine positive Zahl, die so genannte Präferenz, zugeordnet. Wenn mehrere Mail-Exchanger für einen Host existieren, versucht der MTA, die Nachricht an den Mail-Exchanger mit dem niedrigsten Präferenzwert

auszuliefern. Wenn dieser Versuch fehlschlägt, probiert er einen Host mit einem höheren Wert. Ist der lokale Host selbst ein Mail-Exchanger für die Zieladresse, darf er Nachrichten nur an Mail-Exchanger mit niedrigerer Präferenz als seiner eigenen ausliefern. Diese Einschränkung verhindert, dass sich eine Mail zwischen verschiedenen MX-Records in einer Schleife verfängt. Existiert kein MX-Record für eine Domain (oder kein passender), kann der MTA ermitteln, ob zu der Domain eine IP Adresse existiert, und den Versuch unternehmen, die Mail direkt an diese Adresse zu senden.

Angenommen, eine Firma namens Foobar GmbH möchte, dass alle anfallenden Mails von ihrem zentralen Server namens `mailhub` bearbeitet werden. Dann wird sie für jede ihrer Maschinen einen MX-Record wie diesen im DNS eintragen:

```
green.foobar.com.      IN      MX      5      mailhub.foobar.com
```

Das macht `mailhub.foobar.com` als Mail-Exchanger für die Domain `green.foobar.com` mit einer Präferenz von 5 bekannt. Ein Host, der eine Nachricht an `joe@green.foobar.com` ausliefern will, findet im DNS den MX-Record, der auf `mailhub` zeigt. Wenn er keinen anderen MX-Record mit einer kleineren Präferenz als 5 findet, wird die Nachricht an `mailhub` übertragen und von dort an `green` versendet. Soweit in groben Umrissen, wie MX-Records funktionieren. Weitergehende Informationen über Mail-Routing im Internet finden Sie in RFC-821, RFC-974 und RFC-1123.

12.10 Email-Adressen

Genau wie bei der Post müssen auch Emails adressiert werden. Jeder der am elektronischen Austausch von Nachrichten teilnehmen möchte, muss über eine gültige Email-Adresse verfügen.

Email-Adressen bestehen aus mindestens zwei Teilen. Ein Teil ist die *Mail-Domain* (`bbs2.fh-wilhelmshaven.de`), bei der es sich entweder um den Namen des Empfänger-Hosts oder um den Namen einer Maschine handelt, die die Mail im Auftrag des Empfängers bearbeitet. Der andere Teil ist eine Art eindeutige Benutzer-Identifikation, wie der Login-Name des Benutzers oder der echte Name des Benutzers im “Vorname.Nachname”-Format (z.B. Peter Tester) oder ein beliebiger Alias, der zu einem Benutzer bzw. einer Liste von Benutzern übersetzt wird. Andere Adressierungsschemata wie X.400 verwenden einen allgemeineren Satz von “Attributen”, aus denen mit Hilfe eines X.500 Directory-Servers das Empfängersystem ermittelt wird.

Wie Mail-Adressen interpretiert werden, hängt stark davon ab, welche Art von Netzwerk Sie benutzen. Wir konzentrieren uns darauf, wie TCP/IP Netzwerke Mail-Adressen interpretieren.

Aufbau einer Email Adresse (RFC-822)

Internetsysteme halten sich an den Standard RFC-822, der die übliche Schreibweise [user@host.domain](#) verlangt, wobei [host.domain](#) der voll qualifizierte Domainname des Hosts ist. Das Zeichen in der Mitte ist ein “Klammeraffe”; der englische Name “commercial at” (kurz “at”) macht einem eher begreiflich, wieso es als Trennsymbol gewählt wurde. Diese Notation gibt keine Route zum Zielhost an.

Projekttagebuch

06. Februar 2002

Aufbau der Vorläufigen Hardware (3 Standard PC → 1 Server, 2 Clients)
Einbau der Netzwerkkarten
Installation von Red Hat 7.1 (Server und Clients)
Installation von Windows 98SE auf den Clients
Informationsbeschaffung über die Geforderten Teilaufgaben im Internet und aus entsprechenden Fachbüchern

07. Februar 2002

Download von WEBMIN 0.93 und Installation
DNS eingerichtet
Informationsbeschaffung über die Geforderten Teilaufgaben im Internet und aus entsprechenden Fachbüchern

13. Februar 2002

Download von Firewall Builder und Installation
DNS Probleme
Informationsbeschaffung über die Geforderten Teilaufgaben im Internet und aus entsprechenden Fachbüchern

14. Februar 2002

Einrichtung des Time- Server
Einrichtung von Sendmail
Einrichtung der Firewall
Informationsbeschaffung über die Geforderten Teilaufgaben im Internet und aus entsprechenden Fachbüchern

20. Februar 2002

Vorbereitung und Installation von Red Hat 7.2
Kompilierung Apache (mod_proxy)
Informationsbeschaffung über die Geforderten Teilaufgaben im Internet und aus entsprechenden Fachbüchern

21. Februar 2002

Download und Update auf WEBMIN 0.94
Einrichtung Apache
Einrichtung Sendmail
Einrichtung Firewall
Informationsbeschaffung über die Geforderten Teilaufgaben im Internet und aus entsprechenden Fachbüchern

27.Februar 2002

Einrichtung Apache
Einrichtung Sendmail
Einrichtung Firewall
Informationsbeschaffung über die Geforderten Teilaufgaben im Internet und aus entsprechenden Fachbüchern

28.Februar 2002

Einrichtung Apache und 1. Verbindung vom Client
Einrichtung Sendmail
Einrichtung Firewall
Informationsbeschaffung über die Geforderten Teilaufgaben im Internet und aus entsprechenden Fachbüchern

06.März 2002

Endgültige Hardware bekommen ohne redundantes Netzteil
Einrichten der Hardware
Installation von Red Hat 7.2
Einrichtung der RAID- Devices
Anschließen der USV und Installation von PowerChute
Einrichtung der USV (USV- Software darf nicht mit Netzwerkooption auf lokalem Server eingerichtet werden, da sie sonst vom Programm nicht gefunden wird)
Informationsbeschaffung über die Geforderten Teilaufgaben im Internet und aus entsprechenden Fachbüchern

07.März 2002

Einrichtung Apache
Konfiguration der USV
Einrichtung Sendmail
Einrichtung Firewall
Informationsbeschaffung über die Geforderten Teilaufgaben im Internet und aus entsprechenden Fachbüchern

13.März 2002

Einrichtung Apache, aufspielen der Websites der Schule
Einrichtung Sendmail
Einrichtung Firewall
Netzwerkkarte defekt, neue eingebaut
Informationsbeschaffung über die Geforderten Teilaufgaben im Internet und aus entsprechenden Fachbüchern

14.März 2002

Einrichtung von DNS und DHCP, automatische Aktualisierung der Zonendateien nicht möglich, neuere Version des DHCP herunter geladen und installiert
Einrichtung Sendmail
Informationsbeschaffung über die Geforderten Teilaufgaben im Internet und aus entsprechenden Fachbüchern

20.März 2002

Redundantes Netzteil eingebaut, Lüfterplatine angeschlossen, Lüfterbrücke eingebaut
Ergebnis → nichts geht mehr
Fehlersuche Server
Fehler lokalisiert, Lüfterplatine hat Kurzschluss, zwei Lüfter der Lüfterbrücke defekt → wahrscheinlicher Fehlerfall: Durch die zwei defekten Lüfter, wo die Lüfterräder vom Antrieb abgebrochen waren, blockierten die Lüfterräder und es floss ein zu großer Strom. Dadurch entstand auf der Lüfterplatine ein Kurzschluss der wiederum dazu führte, dass das Netzteil abschaltete.
Lüfterplatine und Lüfterbrücke ausgebaut und zum Lieferanten zurück gegeben

21.März 2002

Hinzufügen der User- Zugänge
Aufteilung des Speicherplatzes mit Quotas
Einrichtung Sendmail
Einrichtung Firewall
Informationsbeschaffung über die Geforderten Teilaufgaben im Internet und aus entsprechenden Fachbüchern

17.April 2002

Einrichtung des FTP- Server
Einrichtung Firewall
Erstellung der Dokumentation

18.April 2002

Erstellung der Dokumentation
Testlauf des Servers und Überprüfung aller gemachten Einstellungen

24.April 2002

Erstellung der Dokumentation

25.April 2002

Nochmaliger Testlauf
Überprüfung der Firewall mit einem Portscanner
Erstellung der Dokumentation

02.Mai 2002

Erstellung der Dokumentation

Testlauf des Servers am Netzwerk, Probleme mit DNS, Sendmail und der Firewall

DNS Einträge in der resolv Datei geändert (FORWARDERS)

Bei Sendmail weitere Schnittstelle eingefügt an der Sendmail hören soll

Bei der Firewall die Regeln so abgeändert das Datenverkehr möglich ist

06.Mai 2002

Abgabe der Dokumentation

Literaturverzeichnis und Quellenangaben

Bücher:

Kabir, Mohamed: Red Hat Linux Server – Bonn: mitp Verlag , 2000, ISBN 3-8266-0601-9

Costales, Allman: sendmail kurz und gut – Köln: O'Reilys, 1998, ISBN 3-89721-202-1

Aulds, Charles: Apache Web Server – Düsseldorf: Sybex Verlag, 2001, ISBN 3-815-50322-1

Eilebrecht, Lars: Apache Web Server – Bonn: MITP, 1998, ISBN 3-826-60438-5

Dietrich, Michael: Linux – München: dtv, 1998, ISBN 3-423-50190-1

Links:

www.doc.thepenguin.de

www.abitz.com/Internet

www.linux-as-server.de

www.linuxinfo.de

www.linuxfocus.org

www.linux-community.de

www.fwbuilder.org (Tutorial zum Firewall Builder)

www.tu-harburg.de/dlhp/ (HowTo zu IPTABLES)

www.pl-berichte.de („Firewall selbst entwickeln“)